Prof. Marco Aurélio Thompson

INVASÃO.BR

INVASÕES COMENTADAS PASSO-A-PASSO E EM VÍDEOAULAS

Volume 1

www.cursodehacker.com.br

A forma mais rápida e segura de aprender.

www.hacker.org.br

Prof. Marco Aurélio Thompson

Invasão.BR - Vol. 1

Invasões comentadas passo-a-passo e em vídeoaulas.

2ª edição r2

Projeto Editorial, Diagramação e Revisão: *Marco Aurélio Thompson*
Capa: *Maurício S. de França*

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Thompson, Marco Aurélio
Invasão.BR, vol. 1 : invasões comentadas passo-a-passo e em vídeoaulas / Marco Aurélio Thompson. -- 2. ed. -- Salvador : ABSI - Associação Brasileira de Segurança na Internet, 2005.

ISBN: 85-98941-04-2

1. Computadores - Segurança 2. Hackers de computadores 3. Internet (Rede de computadores) 4. Redes de computadores - Medidas de Segurança I. Título

05-8187 CDD-005.8

Índices para catálogo sistemático:

1. Internet : Invasões : Medidas de segurança : Ciência da computação 005.8
2. Invasões : Internet : Medidas de segurança : Ciência da computação 005.8

O autor e a editora acreditam que todas as informações aqui apresentadas estão corretas e podem ser utilizadas para qualquer fim legal. Entretanto, não existe qualquer garantia, explícita ou implícita, de que o uso de tais informações conduzirá sempre ao resultado desejado. Os nomes de sites e empresas, porventura mencionados, foram utilizados apenas para ilustrar os exemplos, não tendo vínculo nenhum com o livro, não garantindo a sua existência nem divulgação. Eventuais erratas estarão disponíveis no site www.cursodehacker.com.br. O autor também se coloca a disposição dos leitores para dirimir dúvidas e discutir quaisquer dos assuntos tratados nesta obra: por chat, E-Mail, lista de discussão ou telefone.

ABSI - Associação Brasileira de Segurança na Internet
Rio de Janeiro: Caixa Postal: 79.963, Nilópolis, RJ, Cep: 26501-970
Bahia: Caixa Postal: 5017, Salvador, BA, Cep: 40026-970
☎ (21)2231-2899 - (71)8108-7930
Site: www.absi.org.br
e-Mail: atendimento@absi.org.br

ADVERTÊNCIA

As informações contidas nesta obra se baseiam na minha experiência pessoal. Também foram feitas pesquisas na rede mundial de computadores (Internet) e consultas aos relatórios reservados da ABSI - Associação Brasileira de Segurança na Internet. É um livro dedicado a iniciantes e as explicações foram dosadas, para não serem nem demasiadamente técnicas e muito menos superficiais. Enfatizei os aspectos práticos dos temas. A maior parte das técnicas aqui descritas, se colocadas em prática contra terceiros, poderá causar danos, com consequente interpelação judicial. Nosso objetivo ao divulgar estas informações é tão somente o de contribuir para o aumento da segurança nas redes de computadores. Por mais paradoxal que possa parecer, acreditamos que só através da divulgação das falhas existentes nos sistemas de redes locais (LANs) e da rede mundial de computadores (Internet) é que os fabricantes de software, hardware e profissionais de TI se preocuparão em oferecer produtos e serviços comprovadamente seguros. Não concordo com a forma atual como somos tratados enquanto consumidores: empurram-nos programas, produtos e serviços ainda em fase de testes e nos cobram por isto. Esta é a minha bandeira. Em todo caso, me isento da responsabilidade pelo mal uso destas informações. Se em qualquer parte da leitura deste livro, alguma frase, palavra, parágrafo, imagem ou expressão, sugerir o incentivo à prática de delitos, por favor queira desconsiderar a informação. Embora a Constituição Federal, em seu Artigo 5º, me garanta a liberdade de expressão, não dá aos meus leitores e alunos o direito de cometer atos ilícitos a partir das informações obtidas por meu intermédio.

Salvador, 17 de junho de 2005.

Prof. Marco Aurélio Thompson

Sobre o Autor

Marco Aurélio Thompson é carioca, nascido na cidade do Rio de Janeiro. Atualmente é cidadão do mundo e mora onde estiver bombando, com praias, bom tempo e belas garotas. As últimas notícias do seu paradeiro o localizaram em Salvador (BA), próximo a praia de Ondina e do Farol da Barra, projetando sua futura morada, um *Loft* em alguma orla nordestina. Mas quando você estiver lendo este livro ele já poderá estar morando em qualquer outro lugar, desde que seja *cool*.

Desde criança já demonstrava interesse e curiosidade pelas artes, ciências e tecnologia. Fotógrafo desde os treze anos e técnico em eletrônica aos quatorze, foi naturalmente envolvido pela informática através da leitura das revistas técnicas que abordavam o assunto, como a extinta *Nova Eletrônica* e as - ainda nas bancas - revista *Eletrônica* da Editora Saber (*www.sabereletronica.com.br*) e *Antenna-Eletrônica Popular* (*www.anep.com.br*).

Começou a programar em Basic e Assembler em um micro Sinclair (TK-85) e mesmo antes da existência dos cursos regulares de informática, já ensinava os primeiros passos aos seus companheiros de caserna. De quebra, hackeava o telefone público do batalhão. Isto durante os dois anos em que prestou o Serviço Militar no 25º Batalhão de Infantaria Pára-quedista (RJ).

Após a baixa no Exército, ingressou na Polícia Rodoviária Estadual, iniciando na cidade de Ituiutaba (MG) o embrião de um projeto de democratização da informática.

De volta ao Rio de Janeiro começou a colaborar com a revista *Antenna/Eletrônica Popular*, com artigos e programas sobre eletrônica e informática. Nesta época iniciou por conta própria estudos sobre Administração, PNL (Programação Neurolinguística), Gestalt, Eneagrama, Técnicas de Pensamento Lateral, Metafísica, Filosofia, Emotologia, Prosperidade, Aviação Civil e outras formas de autoconhecimento, autoaperfeiçoamento e superaprendizagem.

Em 1989 projetou e operou com uma pequena equipe de colaboradores a *TV Fareua - Canal 3*, primeira TV comunitária a atuar no município de Nilópolis (RJ). Na época ele não imaginava que antes de 2010, cada cidadão poderá ter seu próprio canal de televisão pela Internet.

Em 1995 voltou a se dedicar à democratização da informática e implantou definitivamente o PROJETO INFO 2000 - Informática Para Todos, começando em Nilópolis (RJ) e depois expandindo para a capital. Foram mais de oito mil alunos formados nos quase seis anos do projeto, inclusive nas cidades de Salvador (BA) e Coari (AM).

Pouco tempo depois foi eleito presidente da SBET - Sociedade Brasileira de Educação para o Trabalho (*www.sbet.org.br*), e assumiu também o cargo de Diretor do CET - Centro de Educação para o Trabalho.

Em 1997 tornou-se consultor pelo Sebrae (RJ) e desde então vem orientando empresas e pessoas sobre como obter melhores resultados sob quaisquer circunstâncias.

Em 1999 organizou e fundou com duzentos de seus alunos e ex-alunos dos cursos de telecomunicações ministrados pelo CET, duas cooperativas de trabalho, tendo sido indicado e eleito presidente de uma delas. No mesmo ano foi coordenador e instrutor dos cursos de *WebDesign* da ESTI - Escola Superior de Tecnologia da Informação e instrutor dos cursos de *WebDeveloper* da mesma instituição.

Em 2002 foi eleito presidente da **ABSI - Associação Brasileira de Segurança na Internet** (*www.absi.org.br*) e lançou pela Editora Érica (*www.editoraerica.com.br*), os livros **Java 2 & Banco de Dados** e **Proteção e Segurança na Internet.** Este último lhe valeu uma participação no programa **Sem Censura** especial sobre a Internet, exibido em 18 de novembro de 2002 em rede nacional. Em 11 de maio de 2005 foi novamente convidado ao programa, para falar das últimas ameaças que atormentavam os correntistas de bancos. Também é autor pela mesma editora, do livro **Windows Server 2003 - Administração de Redes**, lançado em 2003.

Em 2003 passou a se dedicar exclusivamente a projetos de minisites. O primeiro deles (*www.cursodehacker.com.br*) se tornou um sucesso tão grande, que obrigou a criação de uma equipe exclusiva para mantê-lo e a seus subprodutos.

Em 2004 lançou pela ABSI **O Livro Proibido do Curso de Hacker** e **O Livro Vermelho do Hacker Brasileiro.** Em dezembro inovou mais uma vez e lançou a revista digital Hacker Brasil (**Hacker.BR**), com distribuição gratuita pela Internet e o DVD **Ação Hacker**, inaugurando a produtora recém adquirida pela ABSI. Ainda para 2005 novos lançamentos estão programados, incluindo o livro definitivo sobre o assunto, a **Bíblia Hacker**, e o mais esperado de seus cursos: o **Curso de Phreaker** (*www.cursodephreaker.com.br*), com a **Bíblia Phreaker** que o acompanha.

Para 2006 outros projetos estão saindo da gaveta, como os cursos de **Cracker de Software**, **Criação de Vírus e Trojans**, **Programação**, **Administração de Redes**, **Preparatório para a Certificação Internacional CEH**, e muitos outros. Todos com a qualidade, facilidade de aprendizagem e o bom humor característico do **Prof. Marco Aurélio Thompson.**

Nós da ABSI temos muito orgulho de tê-lo como presidente.

Roberto Moreno

Vice-presidente da ABSI

"Não vim trazer a paz."

Mateus 10.34

[Ingl., substantivo de agente do verbo *to hack*, ‘dar golpes cortantes (para abrir caminho)’, anteriormente aplicado a programadores que trabalhavam por tentativa e erro.]

Substantivo de dois gêneros.
1.Inform. Indivíduo hábil em descobrir falhas em sistemas de computação, podendo usar este conhecimento para o bem ou para o mal.

Fonte: Dicionário Eletrônico Aurélio

Sumário

Introdução

Este livro surgiu de uma necessidade: ajudar a entender como as pessoas são invadidas, sem perder tempo com teorias desnecessárias e explicações complicadas. Foi assim que nasceu a coleção **Invasão.BR**, composta de livro-texto e CD com vídeoaulas e programas.

Em grau crescente de dificuldade, cada livro desta coleção vai descrever formas diferentes de invasão. O texto de cada capítulo abrange a teoria mínima necessária e nas vídeoaulas, o leitor poderá comprovar o que está escrito. Além disto, este é um livro de autor vivo e o leitor poderá entrar em contato através do e-Mail **atendimento@cursodehacker.com.br** para sanar dúvidas.

Neste primeiro volume abordarei as seguintes técnicas: invasão sem ferramentas, invasão com Google, invasão com SQL, invasão com Languard, invasão com keylogger, invasão com trojan, invasão com phishing scam, invasão de e-Mail e invadindo o próprio micro.

Apesar deste primeiro volume ser mais voltado ao iniciante, procurei incluir informações úteis a quem já não é tão iniciante assim.

Gostaria de aproveitar para destacar as conexões entre os capítulos. Embora cada assunto seja completo, melhores resultados são observados quando combinamos duas ou mais técnicas na mesma **ação hacker**.

Se o capítulo sobre keylogger é suficiente para explorar o uso desta ferramenta, o potencial de ataque aumenta exponencialmente quando o associamos a técnica do trojan e o disseminamos com técnicas de phishing scam.

É desnecessário dizer que as técnicas descritas se destinam exclusivamente ao estudo e não devem ser usadas para causar prejuízo a terceiros. O direito de saber não lhe dá o direito de fazer. Se mesmo assim você insistir em usar este conhecimento para cometer fraudes e atos ilícitos, a responsabilidade será toda sua.

Capítulo I:

Invasão Sem Ferramentas

Capítulo I:

Invasão Sem Ferramentas

SER hacker é **TER** uma forma de pensar característica. Quem pensa como hacker, age como hacker. Partindo desta premissa, concluímos que um hacker deve ser capaz de realizar ações hacker sem depender do sistema operacional, de ferramentas, de equipamento sofisticado ou conexão por banda larga.

O Hacker Não Depende do Sistema Operacional

Qual o melhor sistema operacional? Windows ou Linux? Não importa a resposta. Um hacker não pode depender do sistema operacional para realizar suas ações. Se o equipamento que possui é uma máquina Windows, ótimo. Se for uma máquina Linux, melhor ainda. Sem falar que um hacker experiente pode acessar uma conta *Shell* em máquina Unix de qualquer máquina Windows e até de telefones celulares com acesso a Web.
Eu sei que o mundo Unix tem as melhores ferramentas de rede já embutidas no sistema operacional e aquele blá blá blá todo que a gente já conhece. Mas você acha mesmo que vai encontrar máquinas rodando Unix tão disponíveis quanto máquinas rodando Windows? É este o ponto. Não depender de um sistema operacional para realizar ações hacker. SER hacker, independente do sistema operacional. Usar o que tem em mãos e conseguir resultados. Não usar como desculpa um recurso indisponível ou as próprias limitações. Você começa a SER hacker na mente.

O menino perguntou ao Hackerteen:
_'V*ocê pode usar meu PC com Windows para ações hacker?*"

Hackerteen respondeu:
_"*Não. Só sei invadir com Linux.*"

O Hacker Não Depende de Ferramentas

Outra dependência que o hacker não pode ter é a dependência de ferramentas:

_*"Com meu CD repleto de ferramentas eu faço de um tudo."*

Quer dizer que sem este CD você faz de um nada? O *hacker* deixa de existir? Se transforma no Popeye sem espinafre? Não é porque as ferramentas nos ajudam que devemos nos tornar dependentes delas. Tanto o Windows como o Linux possuem serviços e comandos suficientes para uma série de invasões. O hacker deve saber se virar sem qualquer ferramenta extra. Ou seja, sentar-se diante do micro e a partir do que tem, alcançar o objetivo proposto na **ação hacker**.
É claro que o hacker vai usar ferramentas. Quem consegue passar sem o Nessus ou o NetCat? O problema não é este. O problema é quando qualquer ação hacker depende de uma ferramenta para ser executada. Faça um teste de suas aptidões hacker respondendo à seguinte pergunta:

_*"Você é capaz de idealizar e executar um plano de ataque sem o auxílio de qualquer ferramenta? Usando somente os recursos nativos do sistema operacional?"*

Se a resposta for **NÃO**, você ainda depende de ferramentas e ainda não deve se considerar um hacker completo.

O Hacker Não Depende do Equipamento

Existe diferença entre realizar ações hacker com um Pentium 100 e um Pentium IV de 64bits? Existe sim, mas a diferença não é tão grande como a diferença de processamento sugere. As principais ferramentas hacker rodam nas duas configurações de hardware. É claro que se houver opção vamos preferir o Pentium IV. É claro que quando se pode escolher, preferimos um notebook Semp-Toshiba no lugar da m#%&@ que é o PC Chips. Mas daí a comprometer a ação hacker é outra história.

Uma comparação que gosto de fazer é a do moleque jogando bola. O mauricinho chega com tênis de marca, bola oficial, camisa de time, joelheira, culeteira e o escambau. Mas quem joga mesmo, geralmente é o mais fodido

do time. Repare que nossos melhores jogadores vieram da m#%&@. É um pessoal cascudo. Joga com qualquer bola. Desde as oficiais até as esburacadas, com o recheio amostra. O mauricinho diz que a bola saiu torta porque a trava da chuteira soltou.

O Hacker Não Depende da Conexão

Qual o melhor hacker? O que usa conexão discada ou banda larga? O melhor hacker é o que raciocinar melhor como hacker. Uma conexão de alta velocidade é tudo de bom. Mas - de novo - não é a condição para o hacker mostrar suas aptidões.
Tirando a porcaria que são as conexões por rádio, qualquer outra serve. Se tiver uma conexão por banda larga, ótimo. Se não tiver, não tem problema. Dá para agir também. O que não pode, o que não dá, é se apegar a qualquer dificuldade, mínima que seja, para justificar o fracasso. Fique atento para você não usar como desculpa do insucesso a falta da ferramenta certa, da máquina certa, da conexão certa ou do sistema operacional adequado. O hacker deve ser capaz de usar o que tem para conseguir o que quer. Melhores recursos tornam a ação mais rápida e precisa, mas a ausência de melhores recursos não deve servir como desculpa.

Entendendo a Invasão Sem Ferramentas

Os dois principais sistemas de fechaduras residenciais são Gorges e Yale. Entre estes dois sistemas, o Yale é o que oferece maior segurança. Antigamente era comum usar a fechadura mais cara - a Yale, na porta da frente. E uma fechadura mais barata e não tão bonita - a Gorges, na porta dos fundos.
Um invasor de residências típico, procura por falhas de segurança. Chaves em baixo do tapete, no vaso de plantas, no basculante por dentro da casa, no batente, no alpendre. Um invasor também pode verificar se a fechadura dos fundos usa o sistema Gorges. Se for o caso e se a chave estiver na porta, com um pedaço de arame e usando uma folha de jornal, será possível derrubar a chave por dentro e trazê-la para fora.
Não, nunca invadi residencias. Mas antes de ensinar informática eu ministrava outros cursos profissionalizantes, entre eles o de chaveiro. E posso garantir que não há segurança na maioria das fechaduras vendidas atualmente.
Se você não está acreditando, é só recordar que o casal

William Borner e Fátima Bernardes (apresentadores do telejornal mais assistido do Brasil) foram assaltados dentro de casa por um invasor. Cadê a segurança do condomínio de luxo onde moram? Famosos e endinheirados, será que não compraram nenhum alarme pra casa?
O que ocorreu é muito parecido com o que acontece nas redes de computadores. Achamos que as grandes empresas estão com suas redes seguras, e quando nos dispomos a analisá-las, descobrimos brechas que permite um mero adolescente fazer grandes estragos.
Como exemplo podemos citar o serviço de hospedagem www.kit.net mantido pelas Organizações Globo (www.globo.com). O hacker conseguia roubar a conta de qualquer pessoa, sem o uso de ferramentas. Bastava a digitação de alguns comandos para ter acesso a página de administração do site hospedado. Quer mais provas de que a equipe de TI desta empresa estava deixando a desejar? Tempos depois o concurso de votação do mesmo Kit.Net também foi hackeado.
Confesso a vocês que ainda tenho por hábito verificar falhas que possam ser exploradas sem ferramentas. Neste capítulo vou mostrar algumas descobertas que fiz. Mas não se baseie nelas. Elas servem apenas como exemplo. O mais importante é você entender o raciocínio para se chegar ao problema. Assimilando isso, também será capaz de encontrar falhas.

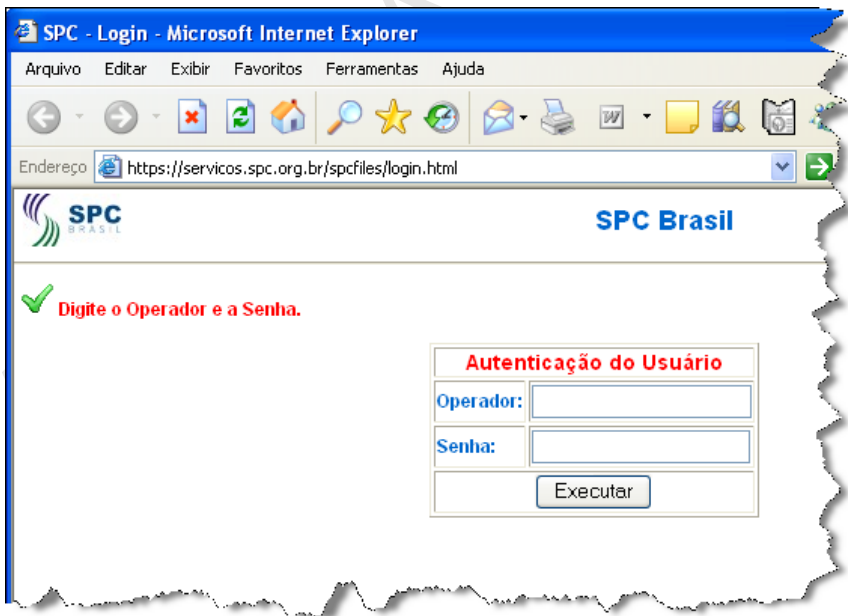
A História do Rei Arthur

Sabe como é a história do Rei Arthur? Existia uma espada fincada na pedra e a lenda dizia que só o futuro rei conseguiria removê-la da pedra. Um rapaz desastrado perdeu a espada do cavaleiro ao qual servia. Procurando por uma espada de reposição, se deparou com a espada fincada na pedra. Ele simplesmente foi lá, tirou a espada da pedra e se tornou o Rei Arthur. Sabe o que eu acho? Que qualquer um teria tirado a espada de lá. Mas só ele teve a iniciativa de fazê-lo.
Na Internet ocorre algo parecido. Alguém se dispõe a verificar a segurança de um site que todos consideram impenetrável e acaba provando o contrário. O site www.voegol.com.br possuía uma falha de segurança que tornava possível visualizar informações dos clientes, caso a compra fosse feita pela Internet. Esta falha já corrigiram, mas deixaram outra que permite consultar a situação do Serasa da pesssoa. Para quem não conhece, o Serasa é um serviço nacional de proteção ao crédito. Trata-se de um cadastro de pessoas com débito na praça. O link a seguir permite que a partir do CPF,

saibamos a situação do SERASA e a data do nascimento. Informando o CNPJ será exibida a data de fundação da empresa:

http://compre.voegol.com.br/serasa/

Além de revelar a situação de crédito, entrega também a data de nascimento do cliente. Para quem conhece os ciclos R+C, inferno astral ou eneagrama, esta informação é um prato cheio.

Você pode encontrar outros sites que permitem tais consultas usando o Google (capítulo 2). Outra forma de consultar bancos de dados dos serviços de proteção ao crédito é visitando as páginas das Câmaras de Dirigentes Lojistas (**CDL**). São dezenas de links, pois existem sites em todos os estados e em várias cidades. Embora a maioria seja de sites seguros, alguns que experimentei permitem consultar dados cadastrais usando injeção de SQL (capítulo 3):

Um outro site permite saber o endereço de qualquer pessoa no Brasil, bastando informar o número de um telefone fixo. Também possui um serviço de consultas ao SPC e SERASA, sendo estes serviços pagos:

O site www.stockphotos.com.br vende pela Internet fotos digitais de alta resolução. É possível ver uma amostra da foto antes de fazer o pedido. Esta amostra vem com uma tarja para inviabilizar o uso. Veja o exemplo:

Bastou analisar o código fonte da página para descobrir como obter a imagem pronta para uso, sem gastar um centavo sequer. São milhares de fotos

a disposição de quem souber como burlar o sistema:

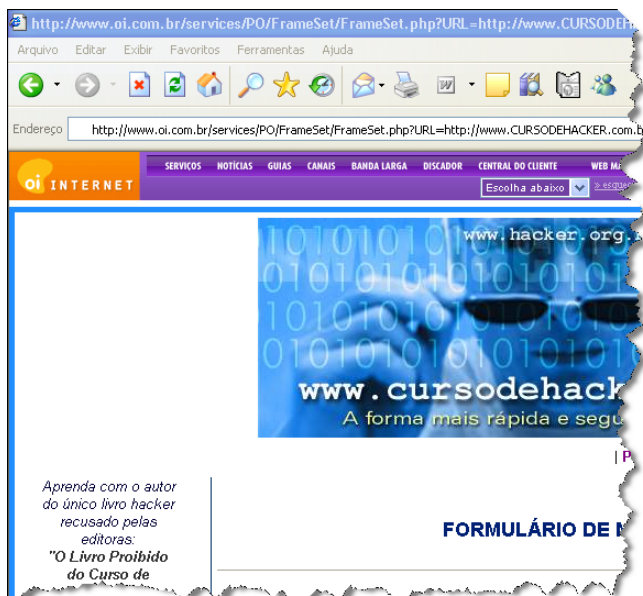
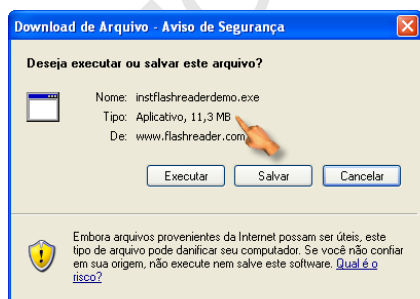
E o que dizer do site do Procon? Que permite ler informações confidenciais dos reclamantes e até excluir reclamações? Outra descoberta simples, onde bastou analisar o código fonte de uma determinada página. Uma pessoa mal intencionada pode enviar correspondência com intimação de pagamento e até se fazer passar por um oficial de justiça ao telefone e obter dados imortantes, como os do cartão de crédito. E agora? Quem vai nos proteger do Procon?

PROCON

Nome: JOSE AUGUSTO
Telefone: 2106-
Endereço: AV. MARIO JORGE
Bairro: SUISSA
Cidade: ARACAJU
Estado: SERGIPE
Empresa Reclamada: NET (TELEVISAO CIDADE S/A)
Telefone: 2107-
Endereço:
E - mail: @redecidade.com.br
Denúncia:
APÓS VÁRIAS TENTATIVAS INFRUTÍFERAS EM SOLUCIONAR
CONTA DE MINHA ASSINATURA, OPTEI POR PEDIR O CANC
05/06/2005.PAGUEI,NESSA DATA, O VALOR DE R$ 52,50 (
CINQUENTA CENTAVOS) REFERENTE A DEBITO A VENCER EM
ME A PAGAR O MES DE JUNHO E OITO DIAS DO MES
CANCELAMENTO DA ASSINATURA, O QUE FIZ EM 25/07/

PROCON

Nome: Sara Alves Santos
Telefone:
Endereço:
Bairro: Ponto Novo
Cidade: Aracaju
Estado: Sergipe
Empresa Reclamada: HiperCard
Telefone:
Endereço:
E - mail: @yahoo.com.br
Denúncia:
Gostaria de saber se pra cancelar qualquer cartão de cr

O site www.oi.com.br permite chamar uma página externa como se fizesse parte do site principal. Não é sem motivo que a prática do phishing scam tem aumentado a cada dia:

Em um determinado site é vendido um certo programa e antes da compra é possível baixar uma versão de demonstração. Mas se fizermos uma pequena alteração na URL é possível baixar o programa completo:

Como a Troca de Parâmetros Pode ser Útil nas Invasões Sem Ferramentas?

Se você não conhece ASP, PHP ou formulários em HTML, é preciso que eu esclarecer uma coisa. Algumas páginas Web recebem informações do usuário e repassam a outra página. Este processo é chamado de passagem de parâmetros. Conhecendo HTML, JavaScript, ASP, PHP e linguagem SQL, você saberá tudo o que precisa para descobrir vulnerabilidades em sites e experimentar invasões sem ferramentas. Existem formas mais sofisticadas de invasões sem ferramentas envolvendo shell script em Linux. Mas este assunto exige mais do que nos prompomos nas páginas deste primeiro volume.

Abaixo segue uma lista com os tipos de páginas que passam parâmetros:

- Páginas de login e senha
- Páginas com formulários, incluindo os de compras online
- Páginas que geram boletos bancários
- Páginas de pedidos
- Páginas com cálculo de produtos
- Páginas que geram cupons e ingressos online
- Páginas de download

As formas mais comuns de passar parâmetros são pelo método GET e pelo método POST. Quando usamos o método POST, os parâmetros estão ocultos ao passar de uma página a outra. E quando a opção é pelo método GET, os parâmetros são exibidos na URL. Para burlar parâmetros via GET é só ler a URL e fazer a alteração necessária. Na figura abaixo temos um exemplo de boleto bancário fraudado. Empresas que trabalham com boletos devem ficar atentas para prevenir este tipo de golpe:

RECIBO DO SACADO

o Número / 88050300-5	Vencimento 21/10/2005
ero Documento 503	Valor do Documento 74,80
Mora / Multa	(=) Valor Cobrado

RECIBO DO SACADO

o Número / 88050300-5	Vencimento 21/10/2005
ero Documento 503	Valor do Documento 7,40
Mora / Multa	(=) Valor Cobrado

Para burlar parâmetros com POST, devemos ler o código fonte da página e procurar pela linha onde está o comando ACTION. Quando sabemos o que está sendo passado e qual página que vai receber as informações, em alguns casos é possível adulterar os parâmetros. Estes são alguns exemplos do que é possível fazer:

- Obter acesso a áreas restritas de sites, seja com a descoberta do login/senha ou fraudando o sistema para que qualquer log in/senha seja aceito
- Alterar valores de compras, pagando menos ou se autoisentando do frete
- Alterar valores e datas de vencimento nos boletos
- Fraudar pedidos online, principalmente os que são totalmente automatizados
- Burlar páginas de cálculos online, impondo o resultado mais adequado aos interesses do fraudador
- Gerar cupons e ingressos sem o devido pagamento ou com características melhores do que as realmente contratadas
- Fazer download de programas, mesmo sem o devido pagamento
- Contratar serviços online dos mais diversos tipos
- Usar endereço de sites conhecidos para abrir páginas armadilha (cross site scripting)

Não existe fórmula única para se chegar ao objetivo nas invasões sem ferramentas. Como exemplo, gostaria de citar o caso de uma empresa que age na fila de marcação de entrevistas da Embaixada Americana. Eles cobravam entre 200 e 400 reais para quem quisesse furar a fila do visto. Não optar por este jeitinho, pode resultar em semanas de espera até a data da entrevista. O que estes fraudadores fazem é agendar entrevistas online usando avatares e laranjas. E quando vendem o 'lugar', cancelam um dos cadastros, incluindo o nome de quem contratou o serviço. Poderiam ser chamados de hackers, mas não são.
Quem conhece programação para a Internet vai encontrar mais facilidade nas invasões sem ferramentas. Quem ainda não consegue pensar como um hacker, talvez se depare com diversas possibilidades de uso da técnica e não consiga enxergar nenhuma.

No CD que acompanha este livro você encontra vídeoaulas com os exemplos citados.

Capítulo 2:

Invasão com Google

Capítulo 2:

Invasão com Google

O Google pode ser acessado por nós brasileiros a partir de dois endereços principais:

http://www.google.com
http://www.google.com.br

Nota: A pronúncia da palavra Google é 'gugou'.

Para acelerar a exibição do resultado, as buscas são feitas prioritariamente na base de dados do idioma local e na americana. Vai deixar de fora outros países. Para ter acesso a resultados diferentes, você deve experimentar o Google em outros idiomas. Este recurso é útil quando o hacker pretende invadir um servidor de outro país ou quando busca por recursos hacker pouco comuns. Um exemplo é a busca de hospedagem gratuita em países exóticos, recurso usado por scammers para dificultar o rastreamento de um site de phishing.

Para acessar a interface em outros idiomas, basta fazer a digitação da URL do país desejado. A lista abaixo tem algumas:

Itália - http://www.google.it
Portugal - http://www.google.pt
China - http://www.google.ch
Argentina - http://www.google.com.ar
Espanha - http://www.google.es
Japão - http://www.google.co.jp
EUA - http://www.google.us

Ou então acessar o link **Preferências** que se encontra à direita, na página inicial do Google. Ainda na página inicial, temos as seguintes opções de pesquisa:

Web - é a busca padrão e a mais usada, que retorna links para arquivos, pastas, páginas e sites na Internet.

Imagens - é usada para procurar figuras e fotos a partir do nome. Use idiomas diferentes para a mesma imagem e conseguirá um resultado mais completo. Se busca pela figura de uma bola, poderá usar bola, ball, sfera,

Grupos - nesta opção você busca mensagens na Usenet, um dos mais antigos sistemas de grupos de discussão da Internet. As mensagens postadas datam do início da Internet e aqui encontramos até o primeiro e-Mail do Linus Torvalds falando sobre um certo 'projeto pessoal de sistema operacional'.

Diretório - nesta opção as informações estão agrupadas por assunto. É útil quando procuramos por temas e não por palavra-chave.

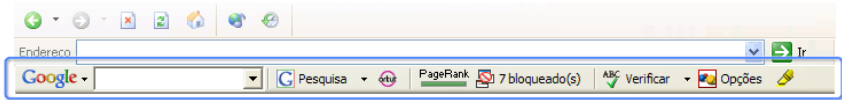
Pesquisa Avançada - aqui você pode montar estruturas de busca mais precisas. Este recurso é útil quando o resultado da consulta é exagerado (retorna milhares de links) e queremos enxugá-lo.

Preferências - aqui você define quantos links serão exibidos por página, o idioma da interface e o idioma das buscas. Também decide se o resultado será exibido na mesma página ou em página diferente.

Ferramentas de idiomas - aqui você pode traduzir palavras, pequenos textos ou páginas Web completas. Uma dica: quando precisar traduzir do alemão para o português, como não existe a opção de tradução alemão-português, traduza primeiro para o inglês e depois use a opção inglês para o português. Perde-se um pouco do texto original na tradução, mas dá para quebrar o galho.

Os botões de busca são dois **[Pesquisa Google]** que é o que todo mundo usa e o **[Estou com sorte]** que vai te levar para uma indicação do próprio Google, relacionada a palavra pesquisada.

Barra de Ferramentas Google

Você pode instalar no Internet Explorer uma BARRA DE FERRAMENTAS Google a partir do link **http://toolbar.google.com/intl/pt-BR/**:

Além do campo para buscas diretas, outros recursos estão presentes, como o bloqueador de pop-ups e o sistema de ranking para os sites. Pense bem se existe necessidade de instalar uma barra de ferramentas Google no seu Internet Explorer. Não deixa de consumir preciosos recursos do sistema e um eventual *bug* pode expor seu micro a invasores.

Google Alert

O Google possui um sistema automático de notificação. Receba em seu e-Mail mensagens de alerta toda vez que um assunto ou palavra-chave for incluída na base de dados do Google. Você pode usar este serviço para se manter atualizado sobre a inserção de algum tema específico: **http://www.google.com/alerts**.

Buscador de Copyright

Este serviço usa o Google para buscar páginas que copiam o conteúdo de outras páginas sem autorização: **http://www.copyscape.com**. Exemplo de uso: o mais óbvio é para saber se alguém está copiando os textos do seu site. Mas não é um serviço 100% confiável para páginas em português.

Origem do Google

O Google surgiu a partir de um projeto de dois jovens estudantes da Universidade de Stanford. Sergey Brin, então com 23 anos, especialista em desenho de aplicativos Web e graduado em Engenharia Eletrônica e Larry Page, então com 24 anos, expert em tratamento de dados e licenciado em informática e Ciências Matemáticas. Eles se conheceram em 1995 e co-

meçaram a desenvolver um algorítmo para extrair informações de grandes volumes de dados. O projeto inicial se restringia a base de dados da Biblioteca Digital da Universidade de Stanford.
Pouco tempo depois começaram a trabalhar em um motor de buscas que varresse a Internet e organizasse as informações em forma de links para as páginas Web. Este sistema começou a funcionar em 1996, com o nome de Backrub. Era um sistema baseado em java e rodava em algumas máquinas Sun e Intel, instaladas na universidade.
O nome Google só surgiu em 1997, ano em que o projeto deixou de utilizar as máquinas da Stanford e foi transferido para o quarto de um dos rapazes, o Larry. No final de 1998 a empresa Google Inc. foi oficialmente fundada, graças a um aporte financeiro de mais de um milhão de dólares doados por amigos e parentes. Perceba que não foi apenas ‘sorte’ e ‘tecnologia’ os responsáveis pelo sucesso do Google. Com quase três milhões de reais as chances de um projeto vingar aumentam bastante, ainda mais quando se trata de uma boa idéia.

Nota: Esta ‘vaquinha’ feita pelos amigos, parentes e investidores, recentemente trouxe problemas para a empresa, pois ao tentar vender ações no mercado de capitais, privilegiaram os antigos colaboradores com ações subsidiadas. Isto é um golpe baixo. Foi descoberto a tempo e o lançamento da Google S/A teve que ser adiado até a poeira baixar.

A Google investiu pesado em pessoal e usa um sistema de trabalho diferenciado que permite aos seus funcionários, uma vez por semana, trabalhar em projetos pessoais. Um destes projetos de funcionários é o Orkut, uma rede de relacionamentos que se tornou febre em pouco tempo. Sistemas como o Orkut já existiam a bastante tempo, mas a Google adquiriu o que eu chamo de ‘toque de Midas’ e tudo o que toca vira ouro.

Significado do Nome Google

A palavra Google é um termo forjado, retirado do termo googol, inventado pelo Dr. Edward Kasner da Universidade de Columbia. O Dr. Kasner queria batizar com um nome sonoro e fácil de recordar, a centésima potência do número 10, ou seja, o número 1 seguido de 100 zeros. Veja como fica:

10000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

Este número é tão grande que supera o número de grãos de poeira existentes no universo. Parece que só serviu mesmo para inspirar o nome Google.

O Que é um Motor de Busca?

O Google é um sistema do tipo **motor de buscas**. Um motor de buscas é um programa de computador que visita site por site da Internet e classifica todas as informações encontradas. Na verdade ele não visita 'um por um'. São milhares de visitações simultâneas. O sucesso de um programa deste tipo está na qualidade do seu algoritmo, um conjunto de instruções que orientam sobre *como* e *o que* procurar.

Praticando...

Vamos conhecer alguns comandos do Google. A maioria destes comandos tem seu potencial ampliado quando combinados com outros comandos, outras palavras ou outros operadores. Darei alguns exemplos, mas não se limite a eles:

[**site:**] Busca restrita ao site especificado. Exemplo de uso:

site:cursodehacker.com.br senha

[**filetype:**] Busca arquivos com a extensão especificada. Exemplo de uso:

filetype:mdb cadastro

O exemplo acima retorna as páginas que contenham o arquivo de nome **cadastro** e seja um banco de dados da Microsoft (MS Access, que gera a extensão **.mdb**). Experimente outras extensões: TXT, PDF, DOC, XLS, DBF, PPT, RTF, MP3, WAV, MID, WRI, etc... Pessoas maliciosas podem obter bancos de dados com números de cartões de crédito usando apenas esta frase de busca.

[**link:**] Busca os sites que tem links para o site especificado.

link:cursodehacker.com.br

O exemplo acima retorna as páginas que apontm para o endereço especificado. Lembre-se de digitar os comandos do Google em minúsculas.

[**cache:**] Busca por páginas antigas do mesmo site, armazenadas em

'cache'. Em sistemas vulneráveis exibe o código fonte das páginas ASP e PHP, mas é uma situação cada vez mais rara. Exemplo de uso:

cache:cursodehacker.com.br

[**intitle:**] Busca as palavras especificadas que estejam no título da página. Exemplo de uso:

intitle:.com.br login

[**inurl:**] Busca as palavras especificadas que estejam no endereço da página (URL). No exemplo abaixo podemos encontrar sites que possuam a mesma falha da empresa de telefonia descrita no capítulo um:

inurl:frameset.php?URL=

A diferença entre este comando e o anterior é que **intitle** busca na TAG TITLE da página HTML e **inurl** busca na URL (o endereço do site).

Operadores no Google

Sistemas informáticos utilizam a lógica booleana. A base da lógica booleana é a seguinte:
- um valor deve ser VERDADEIRO [OU] FALSO
- um valor não pode ser VERDADEIRO [E] FALSO.

Isto parece óbvio pois no mundo dos homens temos o TALVEZ que tanto pode representar VERDADEIRO ou FALSO. Mas no mundo dos computadores não existe lugar para TALVEZ, somente para SIM ou NÃO, Verdadeiro ou Falso.

Os computadores se baseiam na passagem ou não da corrente elétrica, que se compara a uma lâmpada acesa ou apagada. Usamos a matemática para representar a condição elétrica no tempo (aceso ou apagado, verdadeiro ou falso). Quero dizer com isto que matematicamente o estado verdadeiro é representado pelo 1 e o estado FALSO é representado pelo 0. Não se trata do número 0 ou 1 e sim dos algarismos binários 0 e 1.

Você já deve ter reparado que ao buscar por uma palavra no Google, poderá obter como resultado uma imensidão de links, tornando impossível visitar um a um e sem a garantia de que os primeiros links da listagem levam

mesmo a informação procurada. Para melhorar a qualidade das buscas, devemos usar operadores lógicos e matemáticos.
Só para você ter uma idéia, enquanto escrevia este texto, busquei pela palavra **hacker** no Google e obtive uma lista com 238 mil links em português, que continham esta palavra. Se eu usar três minutos visitando cada ink, vou levar cerca de quinhentos dias para visitar tudo, isto se não parar pra mais nada e contando que não entre mais nenhum site no Google depois disso. É para resolver este tipo de problema que servem os operadores. Mas para usar um operador eu preciso saber exatamente o que quero e cá pra nós, buscar por *hacker* apenas não é muito específico. Por isso mudei minha pesquisa para **curso hacker** e obtive mais de 46 mil links. Visitei os primeiros e não achei o que procurava.
Reformulei minha **frase de busca** para **curso hacker pdf** e obtive uma listagem com 21 mil páginas. Bem menos que as 238 mil iniciais. Só que, após visitar os 40 primeiros links sem encontrar nada de útil, alterei a frase de buscas para **curso hacker filetype:pdf**. Agora sim. Das 375 páginas listadas, a maioria possuía material pertinente. O operador lógico utilizado no exemplo foi o [AND] ou [E] que o Google usa implicitamente. Tanto faz eu digitar:

CURSO + HACKER
CURSO AND HACKER
CURSO HACKER

Para o Google as frases de busca acima representam a mesma coisa.

Operador OR (OU)

Usado para buscar uma expressão OU outra. Exemplo: Quero buscar por curso de hacker OU phreaker. No google a frase de busca ficará assim:

curso hacker OR phreaker

O resultado foi de 46.900 links, infelizmente sem nenhum **curso de phreaker**, já que o nosso ainda é recente e ainda não consta no Google.

Operador NOT (NÃO ou -)

Usado para EXCLUIR de uma busca determinada expressão. Suponha que eu queira saber sobre CURSO DE HACKER que não seja o de minha

autoria. No Google ficaria assim:

curso hacker **NOT** “Marco Aurélio Thompson”

Você reparou no uso das aspas? Usamos aspas no Google para buscar pela expressão exata. Se eu fizer uma busca pelo meu nome desta forma:

Marco Aurélio Thompson

O resultado foi de 3.430 páginas em português. Eu não sou tão famoso assim. É que o Google buscou todas as páginas com **marco + aurélio + thompson**, independente da posição destas palavras no texto. Encontrei páginas com as plavras **marco fudeiro**, **aurelio lobo** e **manuel thompson**, pois contém as três palavras pesquisadas. Usando aspas o retorno será de páginas contendo o nome completo. Agora o resultado foi mais justo e retornou apenas 197 páginas, a maioria com links para livrarias online.

Explorando o Google

A qualidade das suas buscas será proporcional a qualidade das suas **frases de busca**. A frase de busca inclui ou não aspas, comandos concatenados e operadores. Primeiro decida o que deseja e depois converta isto em uma boa frase de busca. Artigos, preposições e outros fragmentos de texto são eliminados automaticamente da frase de busca. Imagine quantas páginas o Google retornaria se incluísse nas buscas a preposição **de**. Eu também não a incluí nos meus exemplos. O Google usa um algoritmo inteligente o suficiente para dispensar o uso de acentos. Buscar por **aurélio** ou **aurelio** dá no mesmo. O Google possui alguns recursos úteis, mas pouco conhecidos. Vejamos alguns deles.

Busca de Imagens

Este recurso nós já apresentamos e pode ser acessado a partir da página inicial do Google. O grande segredo é buscar pela mesma palavra em vários idiomas. Suas chances de conseguir achar a imagem que procura aumentam bastante. Não esqueça que imagens podem ter direitos autorais e se você for usar para trabalhos comerciais, existe o risco de processo por violação de copyright. Parece ser uma possibilidade remota, mas existe.
As regras de consulta do Google valem também para a busca de imagens.

Suponha que eu queira imagens relacionadas a telefones celulares, no formato JPG. Posso usar a frase:

mobile filetype:JPG ou **celular filetype:JPG**

Experimente também o serviço de busca de imagens do Altavista, que por sinal, oferece mais opções de filtro que o Google:

www.altavista.com.br/image/default

Google no Celular

Quem possui um telefone celular com acesso WAP habilitado, pode usar o Google para fazer buscas a partir do celular. O endereço de acesso é:

www.466453.com ou **www.google.com/wml** ou **www.google.com**

Google no Palm

Se o endereço tradicional não funcionar, use este: **www.google.com/palm**

Google News

É um serviço do Google específico para busca de notícias: **http://news.google.com**. As empresas de notícias estão tentando impedir este serviço, pois elas é que têm o trabalho de procurar a notícia e o Google usufrui das informações sem gastar com um repórter sequer.

Google Linux

O Google possui um serviço especializado em buscas sobre Linux: **www.google.com/linux**.

Google Microsoft

Também possui um serviço especializado em buscas sobre os produtos da Microsoft: **www.google.com/Microsoft.html**.

Google Cheats

Como se não bastasse, um serviço específico para buscar códigos de trapaça em jogos: **www.cheatgoogle.com/index.php**.

Booble

Um clone do Google especializado em buscar sites e temas pornográficos (a maioria é de serviços pagos): **www.booble.com**.

Google Calc

Você pode usar o Google como calculadora. Basta digitar a expressão matemática no campo de busca. Se você digitar 10+10 no campo de busca vai obter como resultado 20, que é a soma dos dois números. E não é só isto, tem conversor de medidas e a possibilidade de montar expressões. Saiba mais sobre a calculadora Google no link abaixo:

http://images.google.com.br/intl/pt-BR/help/calculator.html

Google Educação

http://scholar.google.com/

Google Universitário

http://images.google.com.br/intl/pt-BR/options/universities.html

Finalizando, uma página com todos estes serviços e produtos Google relacionados.Visite-a de vez em quando para saber das novidades: **http://images.google.com.br/intl/pt-BR/options/index.html**

Google Yellow Pages

Você pode usar o Google como lista telefônica do tipo páginas amarelas, com recurso de mapa. Infelizmente este recurso não esta disponível para o Brasil. Acesse o link: **http://local.google.com/lochp**. Experimente digitar [Thompson] no campo WHAT e [New York, NY] no campo Where.

Google Fedex

Basta digitar entre aspas e a partir da página normal de busca do Google, o código de 12 dígitos da Federal Express. Exemplo: "**Fedex 999999999999**".

Google Patent

O Google exibe informações sobre patentes. Experimente buscar: "**patent 5123123**"

Google FCC
O Google pode ajudar a identificar o fabricante de um aparelho ou placa de computador através do FCC. Experimente buscar:

"fcc B4Z-34009-PIR"

Google Airplane
O Google exibe informações sobre aeroplanos. Experimente buscar:

"airplane n199ua"

Google Compara a Incidência Entre Palavras

www.googlewar.com

Google Exibe o Mundo Via Satélite
Através do Google Earth você pode visualizar qualquer lugar do mundo através de imagens de satélite. Experimente este serviço. Você não vai se arrepender:

http://earth.google.com/

Outros Serviços de Busca
O Google já conquistou seu lugar no coração dos Internautas. Mas não se prenda a um único fornecedor. O Yahoo! por exemplo, possui uma base de dados maior que a do Google. Use serviços de diversos fornecedores para obter melhores resultados. Experimente também:

www.auxilio-a-lista.com.br
Consulte a lista telefônica de qualquer lugar do Brasil e de vários países do mundo. Muito útil quando estamos na fase de footprinting ou quando temos que localizar o endereço de alguém e só dispomos de um nome.

http://registro.br
Ótima fonte de consulta sobre o DNS dos servidores alvo. Muito usado por haclers e defacers.

www.canufly.net/~georgegg/namehost/
Este serviço revela a lista de servidores de um determinado domínio, incluindo um mapa mundi com a localização do servidor.

www.quediaehoje.net/calendario.asp
Calendários de tudo quanto é tipo. Uso? Caso precise de um álibi, poderá saber exatamente que dia da semana caiu determinada data e o que aconteceu na ocasião.

www.apontador.com.br
O Google Earth deixa a desejar quando precisamos de mapas de ruas. Combine o poder da imagem via satélite do Google Earth com os mapas de rua do Apontador. Muito útil para saber se uma pessoa mora onde realmente diz morar ou se determinado endereço existe.

www.maporama.com/share/
Mapas de vários países.

Obtendo Senhas de Programas no Google

Quando se trata de senhas de programas o melhor é procurar em sites específicos de busca de senhas, como o **www.serials.ws**. Se for senha de servidores, que pode ser a base de um defacement ou invasão de e-Mail, faça a busca por bancos de dados e arquivos do Excel. É só experimentar frases de busca do tipo [**cadastro filetype:MDB**] e todas as variações que tiver em mente. Em pouco tempo o hacker pode conseguir diversas senhas, incluindo números de cartão de crédito.

Invasão com Google

O Google encontra centenas de páginas vulneráveis em poucos segundos. A lista a seguir é de frases de busca que podem ser usadas para achar páginas vulneráveis. A maioria delas vai depender do que você conhece sobre redes e programação para a Internet:

“Index of/” + password.txt
“Index of/” + .htaccess
“Index of/” + passwd
Index of ftp +.mdb allinurl:/cgi-bin/ + mailto

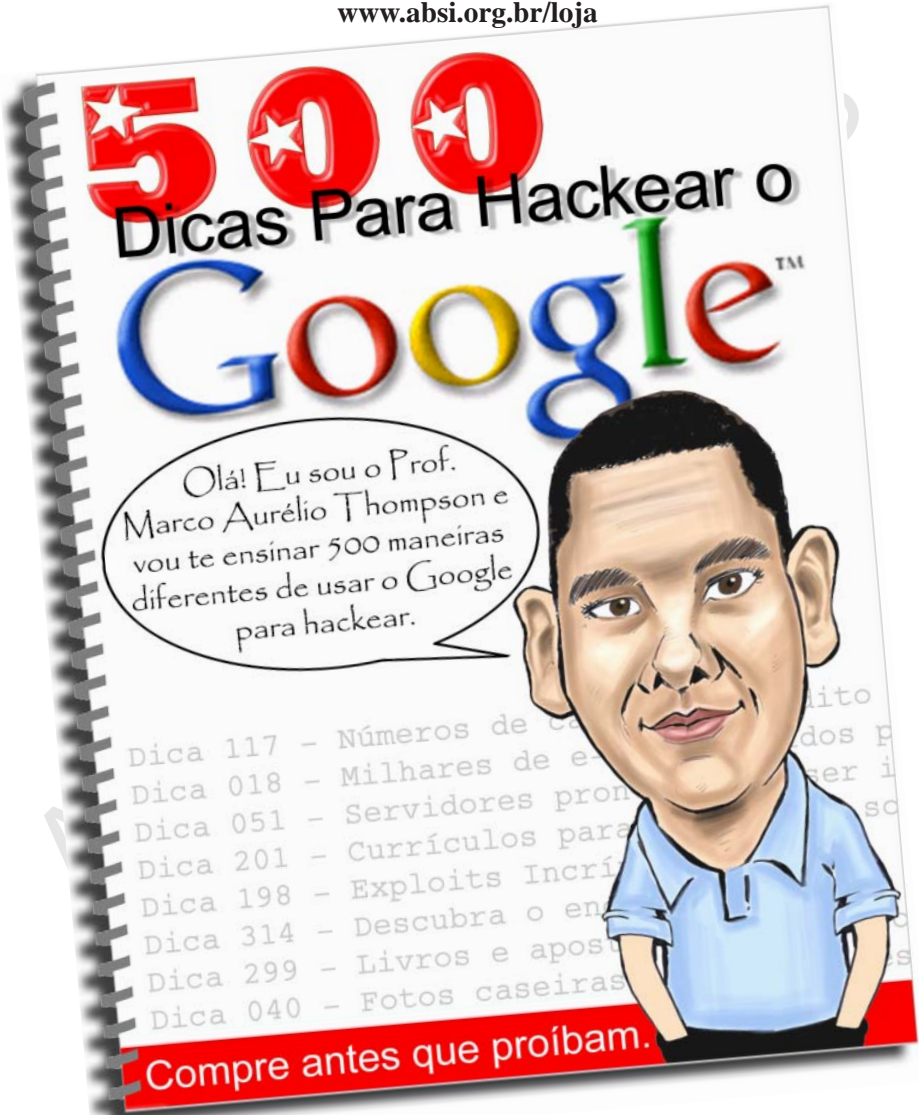
administrators.pwd.index
authors.pwd.index
filetype:config web
inurl:iisadmin
inurl:"wwwroot/*"
inurl:"ftproot/*"
Index of/admin
filetype:htpasswd htpasswd
intitle:"Index of" ".htpasswd" -intitle:"dist" -apache -htpasswd.c
index.of.private (algo privado)
intitle:index.of master.passwd
inurl:passlist.txt (para encontrar listas de passwords)
intitle:"Index of..etc" passwd
intitle:admin intitle:login
intitle:"the page cannot be found" inetmgr (debilidad en IIS4)
intitle:index.of ws_ftp.ini
_vti_pvt password intitle:index.of (Frontpage)
inurl:backup intitle:index.of inurl:admin
"Index of /backup"
index.of.password
index.of.winnt
inurl:"auth_user_file.txt"
"Index of /admin"
"Index of /password"
"Index of /mail"
"Index of /" +passwd
Index of /" +.htaccess
Index of ftp +.mdb allinurl:/cgi-bin/ +mailto
allintitle: "index of/admin"
allintitle: "index of/root"
allintitle: sensitive filetype:doc
allintitle: restricted filetype :mail
allintitle: restricted filetype:doc site:gov
administrator.pwd.index
authors.pwd.index
service.pwd.index
filetype:config web

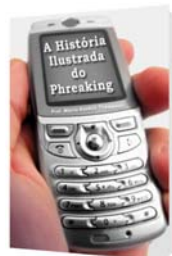
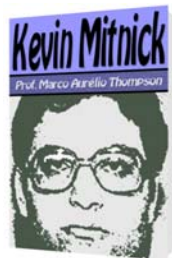
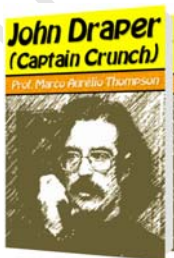
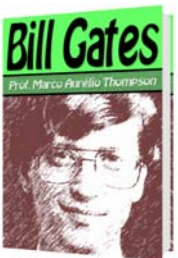
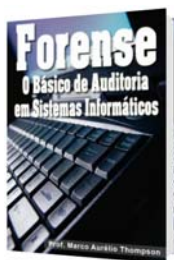
gobal.asax index
inurl:passwd filetype:txt
inurl:admin filetype:db
inurl:iisadmin
inurl:"wwwroot/*."
allinurl: winnt/system32/ (get cmd.exe)
allinurl:/bash_history
intitle:"Index of" .sh_history
intitle:"Index of" .bash_history
intitle:"Index of" passwd
intitle:"Index of" people.1st
intitle:"Index of" pwd.db
intitle:"Index of" etc/shadow
intitle:"Index of" spwd
intitle:"Index of" master.passwd
intitle:"Index of" htpasswd
intitle:"Index of" members OR accounts
intitle:"Index of" user_carts OR user _cart
service.pwd
users.pwd
administrators.pwd
test-cgi
wwwboard.pl
www-sql
pwd.dat
ws_ftp.log
inurl:password.log
intitle:Terminal Server Webs Connection
intitle:Exchange Server login
e-mail address filetype:csv csv
allinurl:admin mdb

Nota: Alguns dos exemplos acima estão explicados nas vídeoaulas do CD que acompanha este livro.

Para saber mais

Se você gostou da possibilidade de hacker sem ferramentas usando o Google, vai gostar do que preparamos para você. O livro 500 Dicas para hackear com o Google traz quinhentas frases de busca prontaspara uso e comentadas. Para fazer seu pedido visite a Loja Virtual da ABSI:

www.absi.org.br/loja

Conheça a Biblioteca Digital da ABSI

www.absi.org.br

Capítulo 3:

Invasão com SQL

Capítulo 3:

Invasão com SQL

Desfazendo a confusão SQL

SQL é a sigla para *Structured Query Language* ou Linguagem de Consulta Estruturada. Uma forma de fazer perguntas a banco de dados usando linguagem de computador. Quando se tem o primeiro contato com SQL é comum as pessoas se confundirem diante das formas que a SQL se apresenta. Não existe uma SQL. Você vai se deparar com:

Linguagem SQL

A linguagem SQL é semelhante a uma linguagem de programação. Só que você não cria programas em SQL. Você cria consultas que são processadas por um servidor SQL ou pelo *engine* de alguma linguagem de programação. Delphi, C++, ASP, PHP, Visual Basic, são exemplos de linguagens que processam instruções SQL.

ANSI SQL

No início da iluminação elétrica, cada fabricante desenvolvia um sistema diferente de lâmpada e receptáculo. A mesma lâmpada vendida como se fosse de 100 Watts, variava pra bem mais ou para bem menos. A rosca poderia ser para a esquerda ou para a direita e o diâmetro também variava, bastando mudar o fabricante. A duração da lâmpada era uma incógnita. Podia durar alguns minutos, horas ou semanas. Meses? Nem pensar.
Com a evolução das relações entre as pessoas surgiram associações que tomaram para si a responsabilidade de sugerir, às vezes impor, a padronização do mercado. A padronização protege o consumidor, ao garantir um padrão mínimo de qualidade nos produtos. Mas também ajuda o fabricante a otimizar seu processo produtivo e vender produtos em outros países.
No Brasil, temos órgãos como o Inmetro (**www.inmetro.gov.br**) e a ABNT (**www.abnt.org.br**) que cuidam da normatização. A ABNT é quem publi-

ca as normas técnicas brasileiras (NBR). As NBRs são documentos com os procedimentos aceitos pelo mercado e órgãos competentes. Algumas organizações conseguem impor padrões ao mercado mundial. A americana **ANSI** - *American National Standards Institute* (**www.ansi.org**) e a alemã **ISO** - *International Organization for Standardization* (**www.iso.org**). Praticamente tudo na indústria da informática é normatizado. Isto inclui as linguagens de programação e também a SQL. Então temos a SQL padronizada que é a ANSI SQL. Acontece que quando uma empresa se torna líder do setor, ela acaba por não acatar 100% da normatização. Empresas como a Microsoft e a Oracle possuem suas próprias versões da SQL. Se você aprende ANSI SQL, SQL na implementação da Microsoft e SQL na implementação da Oracle, vai perceber diferenças entre elas. Neste livro nos referimos a ANSI SQL.

SQL Server

Apesar da maioria das linguagens atuais dar suporte a SQL, existe no mercado ambientes de desenvolvimento e processamento muito mais completos e robustos, conhecidos como SQL Server. Alguns exemplos de servidores SQL são: MS SQL Server, Oracle, MySQL, Sybase e DB2. Quando você aprende sobre um servidor SQL, além da implementação da linguagem com variações da ANSI SQL, aprende também como gerenciar o servidor SQL.

Quem Pergunta Quer Saber

Já vimos que SQL é uma linguagem de consulta. Ela serve para fazer perguntas a bases de dados. Abaixo estão alguns exemplos de perguntas feitas a um banco de dados:

_*"Quantos são os alunos do Curso de Hacker?"*
_*"Quantos são os alunos do Curso de Hacker que moram no Rio de Janeiro?"*
_*"Quantos são os alunos do Curso de Hacker que moram no Rio de Janeiro e são do sexo masculino?"*
_*"Quantos são os alunos do Curso de Hacker que moram no Rio de Janeiro, são do sexo masculino e têm entre 18 e 60 anos de idade?"*
_*"Quantos são os alunos do Curso de Hacker que moram no Rio de Janeiro, são do sexo masculino, têm entre 18 e 60 anos de idade e curso*

superior completo?"
Não a importa a complexidade da pergunta. Se você souber transformá-la em instrução SQL, certamente obterá a resposta.

Onde Estão os Dados?

Antigamente dados e programa eram uma coisa só. Na hora de migrar de um sistema para outro era muito trabalhoso, pois às vezes era preciso reentrar os dados manualmente. Com o tempo surgiu a idéia dos dados separados do código. Os líderes do mercado conseguiram impor seus padrões e os demais fabricantes adotaram filtros de conversão. Este sistema ainda está em uso e você pode importar dados até do antigo dBase III para o MS Access 2003. Este processo de importação não é o ideal. Toda importação oferece riscos e quanto mais antiga for a base de dados, maior é o risco.
O sistema atual mantêm os dados no formato original e o programa faz a leitura sem precisar convertê-los. Isto quer dizer que eu posso ter um arquivo do tipo TXT, MDB, DBX, CSV, DOC, DBF, XLS e um monte de outras extensões e extrair informações destes arquivos sem precisar alterá-los. A SQL poderá ser usada de várias formas, incluindo páginas Web e dispositivos móveis.
Imagine que o Governo Federal crie um banco de dados único, com um número para cada cidadão brasileiro. Vinculado a esta 'conta de usuário', temos todas as ocorrências da vida deste cidadão: todas as notas e anotações escolares, todas as compras que fez, processos em que esteve envolvido como réu ou reclamante, números de todos os documentos, características físicas, foto, impressão digital, código genético e até uma cópia da íris. A partir desta base de dados unificada, será possível saber tudo sobre qualquer cidadão em poucos segundos, bastando 'perguntar' ao banco de dados.
Se o futuro avançar do jeito que está indo, você poderá ser localizado a partir da Internet. Sua identificação poderá ser feita via íris e a localização por GPS. Podemos pensar também em algum tipo de implante sob a pele. Não ria. Em 2005, a novela América da Rede Globo mostrou a personagem Sol sendo localizada pela polícia através de um implante. Satélites poderão exibir sua localização em tempo real. O Google Earth é só ocomeço.
E o que a SQL tem a ver com isso? É que seja agora ou daqui a alguns anos as perguntas continuarão sendo feitas em SQL. Eis um exemplo futurista:
_"Imprima a lista de pessoas que caminhavam pela Rua Trairi, no dia 02

de outubro de 2065, entre 17 e 18 horas, usando calça prata, sapatos aerados e camisa bufante."

Entendeu o que é a SQL? É para extrair informações de bases de dados através de perguntas. É claro que as perguntas codificadas em SQL não são feitas em português. São feitas em SQL. Mas primeiro a pergunta é estruturada em português e depois é codificada em SQL.

Um hacker costuma fazer as seguintes perguntas:

_*"Qual é o nome de usuário do fulano?"*

_*"Qual é o nome e a senha de usuário do fulano?"*

_*"Qual é o número do cartão de crédito do fulano?"*

Em vez de informações sobre pessoas, o hacker pode fazer perguntas do tipo que permita invasões de sistemas:

_*"Qual é a senha de acesso a área restrita deste site?"*

O segredo do sucesso da invasão com SQL é:

- Ter informações sobre a base de dados
- Fazer a pergunta certa

Banco de Dados Relacional

A linguagem SQL é usada para fazer consultas a bases de dados. Isto nós já sabemos. O que veremos agora é o mínimo que precisamos saber sobre bancos de dados relacionais.

SGBD quer dizer Sistema Gerenciador de Banco de Dados. Esta sigla também é usada para fazer referência aos bancos de dados. A expressão 'banco de dados' tanto pode ser usada para se referir ao programa que armazena as informações, como também pode se referir ao arquivo que contém as informações. Vamos usar como exemplo o MS Access da Microsoft, por ser mais simples e provavelmente já estar instalado no seu PC, como parte do pacote MS Office.

Os bancos de dados atuais são do tipo RELACIONAL. São criadas várias tabelas que se relacionam entre si.

Vamos supor que você seja o dono de uma escolinha de natação e precisa registrar seus alunos. A primeira coisa é saber quais informações você precisa sobre cada aluno. Eu suponho que o mínimo para uma ficha cadastral inclua: NOME, DATA DE NASCIMENTO, ENDEREÇO e TELEFONE. Para cadastrar seus alunos você precisará de uma ficha com os CAMPOS acima. Os campos da FICHA CADASTRO não mudam. Então o que muda em cada ficha? Muda as informações de cada aluno. A informação que

mudam a cada FICHA se chama REGISTRO ou TUPLA.

- A etiqueta NOME, IDADE, ENDEREÇO, TELEFONE -> são os CAMPOS
- As informações de cada aluno, como NOME, IDADE, ENDEREÇO, TELEFONE, são os REGISTROS ou TUPLAS
- Um conjunto de CAMPOS forma a TABELA
- Um conjunto de REGISTROS forma o BANCO DE DADOS

Podemos dizer que um BANCO DE DADOS é formado por TABELAS. E as tabelas são formadas por CAMPOS e REGISTROS.
Os bancos de dados atuais armazenam mais que as tabelas, mas por enquanto a definição acima é suficiente. Eu explico como criar bancos de dados na vídeoaula do CD que acompanha este livro.

Praticando SQL

Para praticar o uso das instruções SQL eu sugiro o programa **SQL Tester**, que vai servir como interface gráfica para a entrada dos comandos e permitir a conexão com a base de dados. Por falar em base de dados, disponibilizei no CD um banco de dados criado no MS Access.

SELECT - Usado para consultar dados. A forma mais simples é esta:

SELECT * FROM NomeDaTabela

Em nosso exemplo, vamos digitar assim (para o banco de dados **empresa.mdb**):

SELECT * FROM Clientes

O resultado será a exibição de todos os dados da tabela **Clientes** do banco de dados Empresa.mdb. Para selecionar um ou mais campos da tabela, devemos perguntar assim:

SELECT Nome,Telefone FROM Clientes

O resultado será a exibição apenas dos campos NOME e TELEFONE. Para exibir o resultado em ordem alfabética, usamos ASC:

SELECT Nome,Telefone FROM Clientes ORDER BY Nome ASC

O resultado será a mesma exibição dos campos Nome e Telefone, porém ordenados pelo campo Nome e em ordem crescente. Para ordenar em ordem decrescente usaremos DESC.

Principais Instruções da Linguagem SQL

As principais operações com banco de dados são as seguintes:
PESQUISAR REGISTROS -> aqui você busca informações no banco de dados
PESQUISAR REGISTROS USANDO PARÂMETROS -> aqui você personaliza a pesquisa usando palavras-chave ou curingas
INSERIR REGISTROS -> insere novos registros no banco de dados
EDITAR REGISTROS -> altera os dados de um ou mais registros
EXCLUIR REGISTROS -> apaga do banco de dados um ou mais registros

Em SQL temos as seguintes instruções:

- **SELECT** (pesquisa)
- **DELETE** (exclui)
- **UPDATE** (atualiza)
- **INSERT** (insere)

Para aumentar o alcance das instruções acima, podemos usar a palavra **WHERE** em conjunto com SELECT, UPDATE, DELETE. Esta cláusula permite condicionar pesquisas aos seus critérios de busca. Os exemplos abaixo servem para você praticar um pouco e todos estão comentados nas vídeoaulas do CD:

```
SELECT * FROM Clientes
SELECT * FROM Clientes ORDER BY Nome ASC
SELECT * FROM Clientes ORDER BY DtNascimento DESC
SELECT Nome,Telefone FROM Clientes ORDER BY Nome
SELECT * FROM Clientes WHERE NOT IsNull(Telefone)
SELECT * FROM Clientes WHERE CodCli>2000
SELECT * FROM Clientes WHERE DtNascimento LIKE ‘%1910’
```

Notas:

1) **ASC** quer dizer ordenação ascendente, do menor para o maior. É uma opção padrão e tanto faz usar o comando ASC ou não.

2) **DESC** quer dizer ordenação decrescente, do maior para o menor.
3) **ORDER BY** quer dizer ORDENADO PELO CAMPO.
4) Asterisco **[*]** equivale a TUDO ou TODOS.
5) **IsNull** se refere a campos vazios, sem dados digitados.
6) **NOT** quer dizer QUE NÃO SEJA/NÃO CONTENHA.

WHERE x LIKE

Usamos WHERE quando a palavra pesquisada é única:

WHERE Nome=’João’

Se houver no banco de dados, registros com João + outra palavra, ele não será encontrado. Usando LIKE podemos encontrar a palavra, parte dela ou qualquer expressão, em qualquer parte do registro:

WHERE Nome LIKE ‘%João’ —> procura por João no final do campo.
WHERE Nome LIKE ‘João%’ —> procura por João no início do campo.
WHERE Nome LIKE ‘%João%’ —> procura por João em qualquer parte do campo.

INSERT

INSERT INTO Clientes
(CodCli,Nome,Telefone,DtNascimento)
VALUES
(2222,’Azambuja Frates’,’1234-5678',#01-01-2001#)

A expressão acima insere os valores (2222,’Azambuja Frates’,’1234-5678',#01-01-2001#) nos campos (CodCli,Nome,Telefone,DtNascimento).

Notas:
1) Números entram sem aspas.
2) Strings entram com aspas simples.
3) Datas entram entre **[#]** (tralha ou jogo da velha)
4) O comando pode ser digitado em linha corrida ou partida. Tanto faz digitar em uma única linha, com as instruções uma após a outra, ou da forma que usei no exemplo, com um segmento embaixo do outro.

UPDATE

UPDATE Clientes
SET Nome='Macambuja'
WHERE Nome='Azambuja Frates'

Notas:
1) Na primeira linha temos o comando de atualização informando a tabela.
2) Na segunda linha temos a nova informação a ser gravada no registro.
3) Na terceira linha temos a condição para fazer a alteração, que em nosso caso é o nome ser Azambuja Frates.

DELETE

DELETE FROM Clientes **WHERE** Nome='Macambuja'

Operadores aceitos com WHERE

=	IGUAL A
<>	DIFERENTE DE
<	MENOR QUE
<=	MENOR QUE OU IGUAL A
>	MAIOR QUE
>=	MAIOR QUE OU IGUAL A

Usando NOT (NÃO)

SELECT * FROM Clientes
WHERE NOT Nome='Macambuja'
ORDER BY Nome

No exemplo acima os registros retornados pela consulta são os que NÃO TÊM Macambuja como nome.

Invasão com SQL (SQL Injection)

Já comentei no início do capítulo que a base de dados pode ser acessada via página Web. Usando linguagens de criação de páginas dinâmicas, como ASP, PHP, CFM, Java é possível fazer uma página Web acessar bases de dados. Para pequenos sites a base de dados em MS Access é a mais comum. Bases de dados maiores geralmente são mantidas por servidores SQL, como MS SQL Server e Oracle. Vale a pena destacar o uso do MySQL, cada vez mais comum em sites de diversos portes.

Então o que temos é o seguinte. Uma base de dados que pode ser acessada de uma página Web, disponível a qualquer um na Internet. São páginas de *login* para acesso a áreas restritas do site, acesso a contas por Webmail, consultas a bases de dados, como aquele exemplo da base de dados do Procon que vimos no capítulo um.
A técnica consiste em injetar instruções SQL maliciosas ou mal formadas, com a intenção deliberada de se aproveitar de falhas de proteção na página de consulta. Por isso o nome SQL Injection. Se você não conhece ASP, PHP, HTML, JavaScript e CSS, para melhor aproveitamento da técnica eu sugiro que busque informações adicionais sobre estas linguagens.
Vamos supor uma página de login que peça nome de usuário e senha:

As informações acima são recebidas por um código de programa. Pode ser a mesma página ou uma outra página criada para receber e processar entradas de usuários. É muito provável que o código possua as seguintes linhas:

```
cUsuario = trim(request(usuario))
cSenha = trim(request(senha))
```

Notas:
1) **cUsuario** e **cSenha** são variáveis que vão guardar o nome e a senha digitados a partir da página Web.
2) A função **trim** serve para eliminar espaços em branco digitados acidentalmente antes ou depois do nome ou senha.
3) **Request** é uma função do ASP que recupera as informações do formulário.
4) Não adianta visualizar o código fonte para ler o código em ASP da página de processamento. Os códigos em ASP são processados no servidor e apenas o resultado do processamento será exibido no código fonte.

Na mesma página ASP teremos uma consulta (SELECT) que verifica na base de dados se o Usuário e Senha digitados corresponde a algum cadastro:

```
SELECT usuario, senha FROM Users
WHERE usuario=' & cUsuario & ' AND senha=' & cSenha & '
```

A consulta acima está perguntando se na tabela **Users** existe alguém com o mesmo nome de usuário e senha informados. Após a consulta acima, o programador provavelmente usará um código como este para processar o resultado:

```
If Not objRS.bof Then
        Response.Write 'Seja Bem-vindo' & objRS.fields(nome) & '!'
Else
        Response.Write 'Acesso não autorizado.'
End If
```

O código acima procura até o final da base de dados (BOF). Se os dados digitados baterem com o de alguém cadastrado, o sistema exibe a frase:

Seja Bem-vindo FULANO!

Se os dados digitados não forem encontrados - lembre-se que o nome e a senha deve coincidir com o que está cadastrado, o sistema exibe a frase:

Acesso não autorizado.

Até aí tudo bem. Um código simples e que serve perfeitamente para proteger páginas contra acesso não autorizado. O problema deste exemplo é que ele não possui qualquer tipo de proteção contra entradas mal formadas. Imagine se usarmos a string:

' or '1

(aspas simples + espaço + or + espaço + aspas simples + 1)

A consulta SELECT ficaria assim:

SELECT usuario, senha **FROM** Users
WHERE usuario=’’ or ‘1’ **AND** senha=’1234'

Seria a mesma coisa que perguntar:
‘Retorne o usuário que seja igual a vazio (espaço em branco) ou 1 (um).’ Lembre-se que 1 também representa TRUE/VERDADEIRO. Esta pergunta pode retornar um usuário em branco, que é algo improvável, mas não impossível. Basta lembrar que na fase de construção da base de dados, algum teste pode ter gerado um usuário em branco. Mas na consulta temos também ‘retorne o usuário VERDADEIRO’. Ora, todos os usuários existem, então são verdadeiros. Isto faz com que a consulta retorne todos os usuários da tabela. Só falta pegar a senha. E para pegar a senha é só usar a mesma string **‘ or ‘1** e seguir a mesma linha de raciocínio para compreender o funcionamento. A consulta ficou assim:

SELECT usuario, senha **FROM** Users
WHERE usuario=’’ or ‘1’ **AND** senha=’’ or ‘1’

Que quer dizer: ‘Retorne o usuário que seja igual a vazio (nenhum) OU verdadeiro (todos) E que tenha a senha igual a vazio (nenhum) OU verdadeiro (todos). Isso retorna todos os usuários da tabela, porém com o ponteiro no primeiro usuário.
Quando o programador cria uma tabela de usuários, o primeiro usuário a ser inserido é justamente o administrador. E é exatamente ele que viramos quando exploramos esta falha. Se você já sabe o nome do usuário poderá usar a string **‘ or ‘1** apenas no campo da senha.
Na lista abaixo vemos outras strings que podem ser expermentadas nas invasões com SQL:

‘ or ‘1
‘ or ‘ 1
‘ or ‘1’=’1
‘ or 1=1—
‘or’’=’
‘ or ‘a’=’a
‘) or (‘a’=’a
‘or ‘=1

Procure entender o que cada string ‘pergunta’ ao banco de dados.

Como Encontrar Sites Vulneráveis a Invasão com SQL?

Sendo a porta de entrada as páginas Web que pedem usuário e senha, nada melhor que usar o Google para buscar por páginas de login. Você pode experimentar fazer buscas simples com as palavras USUÁRIO + SENHA ou LOGIN + SENHA ou experimentar buscas como dos exemplos abaixo:

allinurl:admin/index.asp
allinurl:admin/default.asp
allinurl:admin/admin.asp
allinurl:admin/login.asp
allinurl:admin.asp
allinurl:adm.asp

Se você aumentar seus conhecimentos sobre SQL será capaz de construir instruções bastante sofisticadas, o que aumentará as chances de sucesso ao usar a técnica. Veja mais nas vídeoaulas do CD que acompanha este livro.

Capítulo 4:

Invasão com Languard

Capítulo 4:

Invasão com Languard

Languard: O Que é?

O *GFI Languard Network Security Scanner* é uma ferramenta da categoria programa de varredura ou *port scanner*. O uso previsto para o Languard é buscar por vulnerabilidades no próprio micro, na rede local ou na Internet. Mas hackers e curiosos têm usado programas de varredura para buscar vulnerabilidades nos micros e redes dos outros. Um programa de varredura pode buscar por: PORTAS, VULNERABILIDADES e/ou SERVIÇOS (programas em execuçao no micro). O Languard faz todas estas buscas e por ser fácil de usar, é a nossa indicação para quem está iniciando. Quando você estiver mais a vontade com o Languard, sugiro programas com mais recursos como o NetCat e o Nessus. Gostaria de antecipar que estes programas possuem mais recursos mas também são mais exigentes quanto ao seu conhecimento sobre redes e sistemas. Por isso não os recomendamos para iniciantes.

Languard: Onde Obter?

Não sou ingênuo a ponto de achar que os leitores deste livro vão mesmo pagar quase cinco mil reais por uma versão comercial do Languard. Então vamos direto ao ponto. O Languard é fabricado pela empresa GFI Software Ltd (**www.gfi.com**) e você pode baixar uma versão completa, válida por trinta dias, a partir do link: **www.gfi.com/lannetscan/**.
A versão 7 estava disponível quando escrevi este capítulo. Roda em Windows XP, 2000 e 2003. Se você ainda usa o Windows 98 ou Me, vai precisar de uma versão antiga do Languard. É recomedável que você baixe a versão mais atual. Isto garante que a varredura será capaz de lidar com as vulnerabilidades mais recentes.
Após baixar o programa talvez você queira obter um serial válido para fugir da limitação de 30 dias de uso imposta pelo fabricante. Neste link

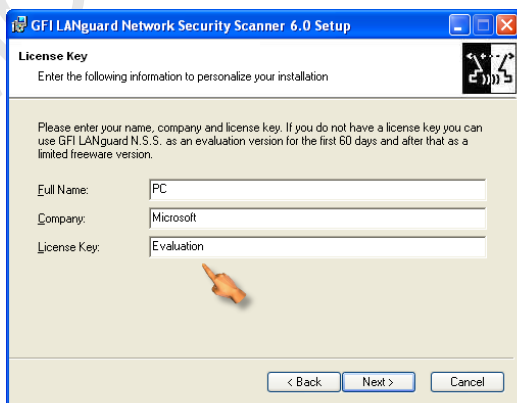
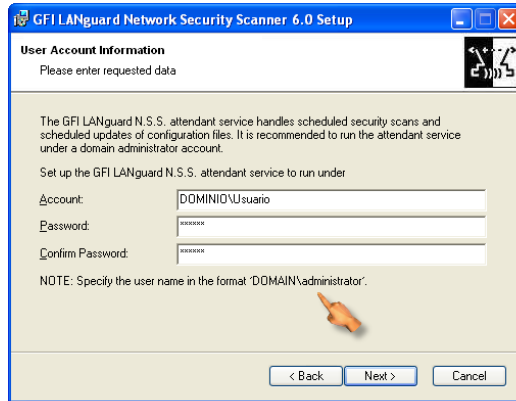
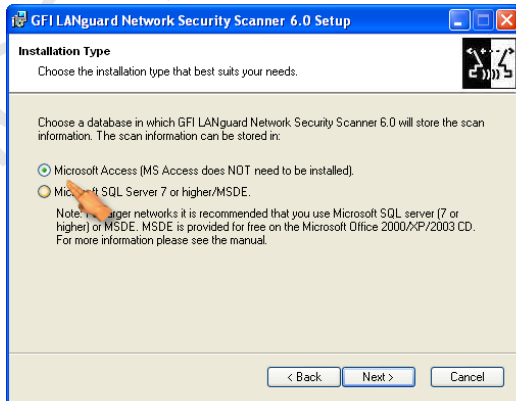
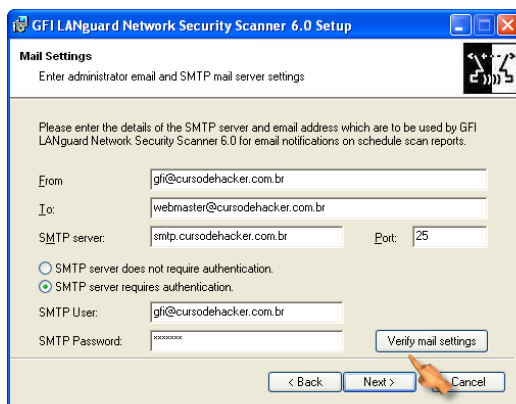
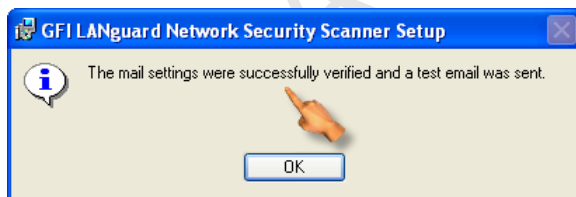
você encontra o serial de vários programas, incluindo o Languard: **www.serials.ws**.

Dois avisos importantes;
1) Desabilite qualquer firewall que esteja usando, pois eles interferem no funcionamento dos programas de varredura.
2) Usuários de Internet por rádio devem optar por conexões *dial-up*, pelo menos durante a varredura.
3) Usuários do Windows XP com SP2 precisam fazer alguns ajustes no sitema para tirar melhor proveito do Languard. Leia um tutorial a respeito em:

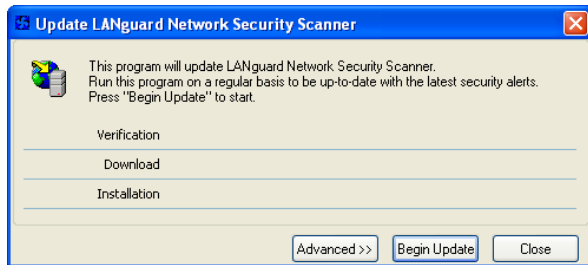
http://kbase.gfi.com/showarticle.asp?id=KBID002177

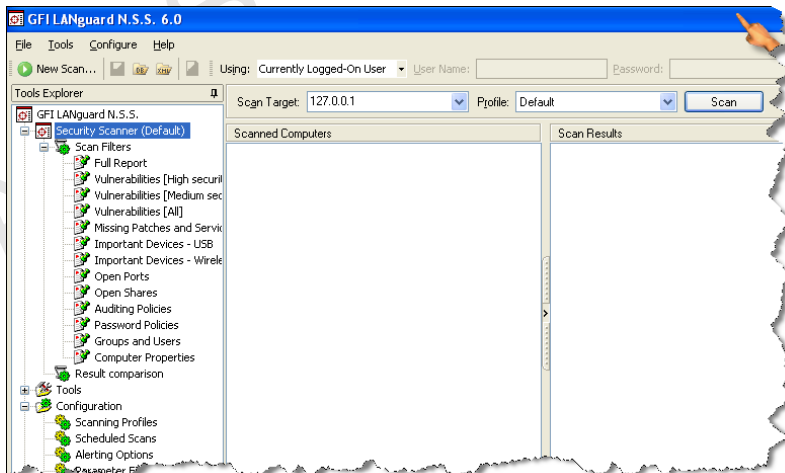
O procedimento consiste na liberação de algumas portas, habilitação e configuração de alguns serviços do Windows XP SP2. Se você ignorar este aviso, o resultado da varredura pode ser nulo ou incompleto.

Languard: Instalação e Configuração

1. O programa que você baixou é completo, válido por 30 dias. Para usar a licença de avaliação é só manter a palavra ‘Evaluation’ como número de série. Se você baixar um número serial e usar, vai ter a mesma funcionalidade da versão comercial, sem o prazo de expiração. Para fazer este capítulo eu usei a versão gratuita, válida por trinta dias. Não levei tanto tempo para escrever e esta validade foi suficiente. Acredite se quiser. ☺

2. No Languard 6 em diante você precisa definir uma conta de usuário logo no início da instalação. Você precisa estar logado no sistema operaconal com direitos de administrador. O mais comum é usar o nome da máquina (domínio) seguido do seu nome de usuário (com privilégios de administrador). Entre com a senha da sua conta no espaço correspondente:

3. Agora você precisa definir qual base de dados será usada pelo Languard. As opções são o MS Access e o MS SQL Server, instalado separadamente. O MS Access é a melhor opção para o iniciante e também para o consultor independente:

4. Na próxima etapa você define a conta de e-Mail que vai receber os relatórios do Languard. As informações solicitadas são as mesmas que você utiliza para configurar uma conta em um cliente de e-Mail:

5. Use o botão de teste para verificar a configuração da conta de e-Mail. Se tudo estiver OK, você receberá a seguinte mensagem do sistema:

7. Após concluir a instalação você tem a opção de começar a usar o programa. E se você estiver conectado a Internet, a atualização da base de dados terá início:

Esta atualização é importantíssima para que o Languard possa identificar as mais recentes vulnerabilidades. Se você não puder ou não quiser atualizar o Languard no processo de instalação, poderá fazê-lo via menu, seguindo a sequência:

Help -> Check for Updates

Languard: Fazendo a Varredura

A varredura é um processo bem simples, pois basta informar o IP ou faixa de IPs a serem pesquisados. A dificuldade que você vai encontrar é na análise do relatório. Descobrir o que fazer com as informações apresentadas depende dos seus conhecimentos sobre redes, protocolos e sistemas operacionais de redes. Na medida do possível vamos dar dicas e orientações sobre as vulnerabilidades mais comuns.

O Languard é uma ferramenta prática. A continuação deste capítulo se encontra nas vídeoaulas do CD que acompanha o livro. Lá você vai aprender a:

- identificar cada uma das opções do programa
- fazer a varredura de uma única máquina, de faixa de IPs e de domínios
- usar as ferramentas de rede embutidas no Languard
- configurar o Languard para redes lentas, IPs que não respondem e máquinas protegidas por firewall
- analisar e comparar relatórios
- explorar as vulnerabilidades mais comuns e
- como lidar com as vulnerabilidades que você ainda não conhece

Capítulo 5:

Invasão com Keylogger

Capítulo 5:

Invasão com Keylogger

Keylogger: O Que É?

Keylogger é um programa que, quando instalado, passa a capturar todos os caracteres digitados no teclado. Os keyloggers evoluíram e além das teclas digitadas, alguns destes programas conseguem monitorar as atividades do computador PC. Isto inclui sites visitados, tempo gasto em cada um deles, imagem ao redor do clique do mouse e cópias da área de trabalho. Os keyloggers atuais são capazes de se instalar remotamente e enviar os dados coletados por e-Mail, FTP, IRC e mensageiros. Os keyloggers atuais deixaram de ser simples capturadores de teclas e se tornaram uma mistura de keylogger + trojan.

O uso lícito do keylogger se dá quando um empregador ou pai zeloso, precisa ter controle sobre as atividades online do filho ou funcionário. Hackers se aproveitam desta característica de monitor e utilizam os keyloggers para roubar senhas, logins, números de contas corrente e cartões de crédito, senhas de e-Mail, enfim, tudo o que for digitado ou mostrado na tela do computador.

Keyloggers são por natureza programas de Script Kids. Um hacker, na verdadeira concepção da palavra, direciona suas ações a micros servidores. Isto não quer dizer que um hacker não possa usar keyloggers como parte de um PLANO DE ATAQUE. Meu comentário diz respeito apenas a natureza deste programa. Não é um programa típico de ação hacker.
O funcionamento básico do keylogger é este: capturar a digitação e gravar em arquivo de texto com extensão .txt ou .log. Os arquivos gerados pelos keyloggers podem ser lidos em qualquer editor de texto. Alguns keyloggers oferecem a opção de critografar o arquivo de log. Keyloggers podem oferecer outras funções, como:
- gravar os mais diversos tipos de atividade no micro, como abertura de

janelas, execução de programas e coordenadas de movimentação do mouse.
- enviar o relatório da monitoria por e-Mail, para um FTP ou serviço de mensagem instantânea, sendo o mais comum o ICQ.
- capturar a imagem ao redor do mouse ao clicar. Um monitor deste tipo pode ser usado para burlar a segurança dos tecladinhos virtuais usados pelos bancos. Alguns bancos somem com os caracteres no momento do clique.
- se instalar a partir de outro programa, tornando o keylogger também um trojan (cavalo de tróia).
Pela lista acima, você pode perceber que existem keyloggers com diversas funcionalidades e disponibilidade de recursos.

Keylogger: Como Usar?
O keylogger do tipo mais simples só precisa de duas operações:

- Fazer a instalação no local
- Analisar os relatórios de LOG de tempos em tempos

Para um keylogger com recurso de aviso remoto é preciso:

- Fazer a Instalação no local
- Configurar a forma de envio do LOG
- Receber e analisar os relatório de LOG de tempos em tempos

Para um keylogger que permita ser instalado remotamente (keylogger com trojan):

- Configurar o servidor
- Camuflar o servidor
- Distribuir o servidor
- Aguardar até que o usuário instale o servidor
- Receber e analisar os relatório de LOG de tempos em tempos

Neste último exemplo as chances de êxito são bem menores. Poucas pessoas tem aberto anexos de e-Mail ultimamente. E se for um keylogger dos mais populares, provavelmente já consta na lista dos principais antivírus e será detectado.

Criminosos que se utilizam de trojan-keyloggers para capturar senhas de correntistas pela Internet, geralmente contratam um programador para desenvolver um programa espião personalizado e menos sujeito à detecção por antivírus.

Keyloggers na Prática

Vamos começar apresentando um keylogger bem simples, é o Home Key Logger. Ao ser instalado ele se copia para a pasta:

C:\Arquivos de programas\HomeKeyLogger

Minha primeira sugestão é que você mude o nome da pasta, pois o nome original informa a natureza do programa. Depois que o Home Key Logger for instalado, ele aparece na forma de ícone na bandeja do sistema, próximo ao relógio:

Clicando com o botão direito do mouse sobre o ícone, você tem acesso as opções de configuração do keylogger:

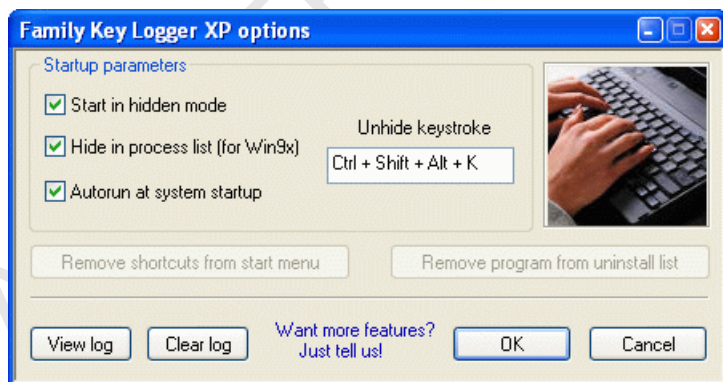
View log
Autorun
Hide icon
Clear log
FAQ
About
Want more
Comments...
Exit

View log -> visualiza a captura.
Autorun -> o programa incia com o Windows.
Hide icon -> esconde o ícone na bandeja. Para voltar a vê-lo, use as teclas CTRL + ALT + SHIFT + M.
Clear log -> limpa o arquivo de log.
Exit -> Encerra o programa.

O arquivo de log é o **KeyLog.txt** e se encontra na mesma pasta em que o programa foi instalado.

Este keylogger é dos mais simples e só serve mesmo para ajudar a entender o funcionamento deste tipo de programa. Com a evolução dos antivírus, é possível que ele seja detectado já na instalação. Um outro problema que vai ocorrer com este keylogger é que ele não captura os sinais gráficos da língua portuguesa. Ou seja, palavras acentudas, cedilhas e outros símbolos e sinais não serão capturados, podendo aparecer como lixo ou espaço. O teclado pode parar de acentuar e agir de forma estranha. Estes problemas ocorrem em praticamente todos os keyloggers antigos e é uma das maneiras que temos para suspeitar de um keylogger em nossa máquina.

O Keylogger na Lista de Tarefas

Além do funcionamento anormal do teclado - não confundir com teclados mal configurados - outra forma de verificar se existe um keylogger instalado na máquina é verificar a lista de tarefas do Windows. Para acessar a lista de tarefas você deve usar a combinação de teclas CTRL + ALT + DEL e verificar os nomes na aba **Processos**. No caso do Home Keylogger vai aparecer o nome do executável que é **keylogger.exe**. Isto pode ser resolvido com a alteração do executável para um homônimo de algum processo do Windows. Os keyloggers mais recentes oferecem a opção de se ocultar da lista de tarefas.

O Que Esperar de um Keylogger?

O keylogger ideal não existe. Está para ser feito e pode ser feito por você, com estudo e dedicação. O keylogger ideal não é só keylogger, ele é um misto de servidor smtp, trojan, keylogger e screen logger (ou grabber).

O problema de um keylogger deste tipo é ele fazer tanto sucesso que acaba sendo incluído na lista de programas maliciosos dos principais fabricantes de antivírus. É isto o que ocorre toda vez que um malware fica famoso: passa a ser bloqueado pelo antivírus. Enquanto você não cria o keylogger ideal, nos daremos por satisfeitos com um keylogger que:

- possa ser instalador no computador local
- envie os dados coletados para nosso e-Mail ou ICQ

Tendo um keylogger com as características acima já será possível executar algumas ações hacker. Um passo além deste keylogger é de um que possa ser instalado a distância. Este tipo é um dos mais difíceis de obter sucesso, uma vez que poucos tem se arriscado a instalar programas desconhecidos em suas máquinas. E a monitoria tem que ser constante. Quem garante que a vítima vai estar com o PC ligado ao mesmo tempo que você? Quem garante que o firewall não vai alertar sobre as atividades do trojan? Não estamos lá pra ver. As chances de sucesso são maiores quando o alvo é indefinido (envio do trojan-keylogger em massa) ou quando é feito o uso combinado com outras técnicas, principalmente o phishing scam e a engenharia social.

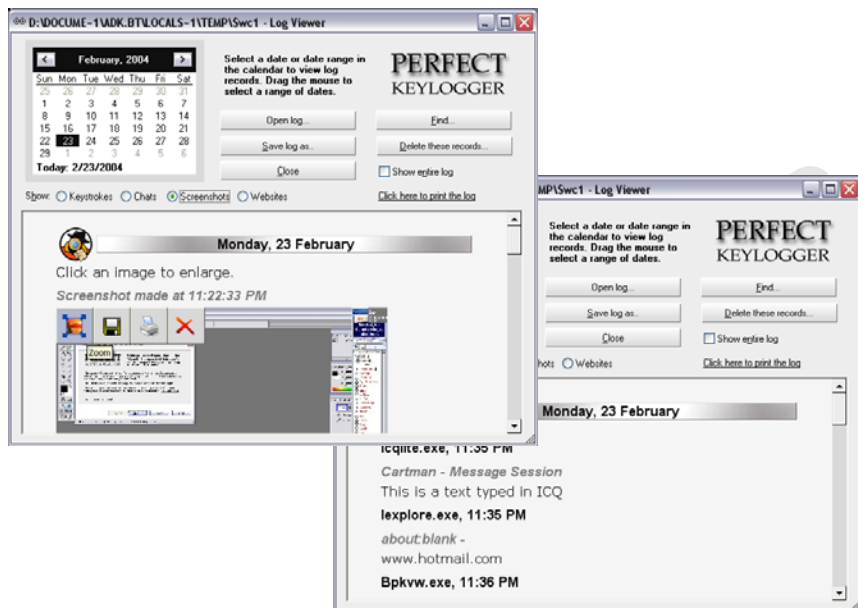
Por fim, temos os keyloggers que capturam telas ou cliques do mouse. Neste caso podemos até usar um programa de captura de tela, como o Snagit (**www.techsmith.com**), que tem a opção de captura temporizada e envio das telas por FTP, ICQ ou e-Mail, inclusive a área em volta do mouse. Como nem tudo é perfeito, este programa não é instalado a distância.

Superkeyloggers

A família dos keyloggers não para de crescer. Além do keylogger específico para monitorar as atividades do micro, a lista deste tipo de programa passou a incluir: Microphone Spy, Phone Recording, Telephone Spy, Webcam Spy, ICQ Logger, AIM Logger, IRC Logger, MSN Logger, Skype Logger, Screen Grabber, NET Video Spy, entre outros espiões. Existem programas que até pelo som das teclas consegue descobrir o que a pessoa digitou.

Keyloggers x Antivírus & Cia

O principal problema dos keyloggers é a detecção pelo antivírus e antispywares. Um exemplo é o Perfect Keylogger, que apesar de ser um programa excepcional, capaz de capturar telas e área ao redor do mouse,

conteúdo de chats e ser instalado remotamente é detectado pela maioria dos antivírus.

Uma agradável supresa tivemos com o KeySpy BR, um keylogger nacional que apesar de possuir menos recursos que o perfect Keylogger e alguns outros programas do tipo, pelo menos por enquanto, está conseguindo burlar a proteção dos antivírus e antispywares.

Problemas com Keyloggers

Os principais problemas que você vai encontrar ao usar keyloggers são os seguintes:

- não conseguir fazer a instalação remota
- não conseguir receber os LOGs por e-Mail, FTP ou mensageiro
- não conseguir ocultar o keylogger do antivírus

Veremos mais sobre como usar os keyloggers e como resolver os problemas acima nas vídeoaulas do CD que acompanha este livro.

Capítulo 6:

Invasão com Trojan

Capítulo 6:

Invasão com Trojan

Trojan ou troiano é a simplificação do nome *trojan horse*, que na tradução para o português significa **cavalo de tróia**. A função do trojan é abrir portas no PC, permitindo a invasão. O trojan é disfarçado na forma de algum arquivo convidativo, como vídeos de apelo sexual, geradores de crédito para celular ou cartões virtuais.

O nome ‘cavalo de tróia’ surgiu em referência a lenda de Tróia que é mais ou menos assim: o rei de Tróia visitou um outro rei, Menelau, e se encantou por sua esposa, Helena. Alguns dizem que ela foi raptada outros dizem que a marvada fugiu com o rei de Tróia. Independente de ser fuga ou rapto, diz a lenda que Menelau, o corno, reuniu um exército e foi a Tróia reaver a mulher. A guerra durou sete anos. Tróia ficava numa posição privilegiada e de difícil acesso. Alguém teve a idéia de fazer um cavalo de madeira para dar de presente como prova da rendição. Os troianos engoliram a isca e botaram o cavalão pra dentro. Como você já deve ter visto na TV ou no cinema, dentro do cavalo de tróia se esconderam alguns soldados do rei Menelau. A noite estes soldados abriram os portões de Tróia e permitiram que o rei Menelau entrasse pra ver o que sobrou da esposa, depois de sete anos de vida sexual com outro.

Como este malware faz exatamente isso, finge ser um presente e oculta código malicioso para abrir as portas do micro, atribuir a este tipo de programa o nome Cavalo de Tróia (Trojan Horse) ocorreu naturalmente.

Os Trojans não se reproduzem, a exemplo dos vírus, mas deixam as máquinas comprometidas bastante vulneráveis.

No Brasil, as ações hacker que mais prejuízos causam as instituições financeiras são ataques de trojans, direcionados a clientes de bancos e operadoras de cartão de crédito.

O trojan é formado por duas partes. Um módulo CLIENTE que o hacker instala na própria máquina, e um módulo SERVIDOR que a vítima deve instalar na máquina a ser comprometida. O módulo SERVIDOR abre o micro comprometido. E o módulo CLIENTE faz a conexão e permite o controle total da máquina invadida. Como ninguém em sã consciência se propõe a instalar programas maliciosos no próprio micro, o hacker usa técnicas de persuasão, conhecidas como ataque de engenharia social. Sendo o trojan um programa escondido em outro, não é difícil convencer o usuário leigo a abrir um suposto cartão virtual, por exemplo.
Apesar da forma mais popular de instalação do trojan ser com a colaboração involuntária de sua vítima, atualmente é possível instalar trojans bastando uma visita à página comprometida.

Trojan na Prática

Devido a natureza do trojan - camuflar programas e códigos maliciosos - é preciso ter cuidado ao baixar este tipo de programa de sites desconhecidos, pois podem ser trojans contendo outros trojans. Ou seja, na intenção de invadir com trojans, o invadido pode ser você. Para eliminar, ou pelo menos reduzir esta possibilidade, incluimos nos CDs que acompanha este livro alguns trojans livres de pragas virtuais.
O segundo ponto a ser observado, tão ou mais importante até que o anterior, é o risco de executar na sua própria máquina o arquivo do trojan que deveria ser executado pelo alvo.
Lembre-se que é o módulo servidor que vai ser enviado e instalado na máquina alvo e é o que vai permitir a invasão.

Trojan: Como Usar?

O uso do trojan segue sete passos distintos:
1. Obter o trojan de fonte confiável
2. Instalar o trojan na máquina local para gerar/configurar o módulo servidor
3. Configurar o módulo servidor
4. Preparar o módulo servidor para distribuição
5. Distribuir o módulo servidor para alvo certo ou aleatório
6. Aguardar que o usuário execute o módulo servidor na máquina alvo
7. Quando a máquina alvo estiver rodando o trojan, é só estabelecer contato

1º PASSO: Obter o Trojan de Fonte Confiável
Além dos trojans no CD que acompanhe este livro, segue abaixo alguns links confiáveis onde se pode obter trojans atualizados:

http://www.trojanfrance.com/index.php?dir=Trojans/
http://areyoufearless.com/

Aluns trojans que vale a pena conhecer:

Trojans antigos e tradicionais:
BackOrificie
NetBus
SubSeven
WinCrash

Mais recentes e com mais recursos (trojans de terceira geração):
Beast
Net-Devil
Optix Pro
Lan Filtrator

2º PASSO: Instalar o Trojan na Máquina Local para Gerar/Configurar o Módulo Servidor
A primeira coisa a fazer é instalar o trojan em sua própria máquina. Volto a lembrar do risco desta operação, pois você poderá executar por engano o módulo servidor e alguns destes programas são de dificil remoção. Se você seguir as instruções da vídeoaula que acompanha este livro, os riscos são menores. Mas em uma expedição que fiz a África, o guia orientou nosso grupo para só atirar em camelos. Mesmo com a orientação, muitos atiraram em dromedários. Ou seja, mesmo com o alerta para não executar o módulo servidor em sua máquina, é possível que por acidente ou curiosidade, ele seja executado. Já passei por isso com um aluno de outro curso, eletriscista predial, que ministrei na quadra da Escola de Samba Acadêmicos do Grande Rio, em Duque de Caxias (RJ). O aluno cismou de curtocircuitar uma tomada só para ver no que dava.
Um excelente nível de segurança pode ser obtido de você fizer todos os testes em máquinas virtuais, criadas especialmente para esta finalidade. Não use ativírus nem firewall na máquina virtual, pois estes programas

podem impedir a instalação do gerador do trojan.
Provavelmente você também receberá mensagens do antivírus quando tentar descompactar os trojans do CD que acompanha este livro. É apenas um alerta, pois o trojan só se instala se o *server* for executado. Mas este alerta pode bloquear a descompactação 'por medida de segurança'. Este é mais um motivo para usar máquinas virtuais na experimentação de trojans.
A esta altura você deve estar se perguntando: se o antivírus detecta o trojan, então não adianta tentar enviá-lo? Será o trojan uma técnica ultrapassada e que não merece mais crédito?
Pelo contrário. O uso de trojans é o que tem causado enormes prejuízos aos bancos e operadoras de cartão de crédito. Confesse aqui no cantinho da página: Quantas vezes, só neste mês, você recebeu mensagens de e-Mail com trojans? Não lembra? São aquelas mensagens com cartões virtuais, cobranças do SERASA, fotos de mulher pelada. Lembrou agora?
Não faz nem um mês que eu estive no programa Sem Censura da TV Educativa/TV Cultura para falar sobre o assunto. Na ocasião o ator da Rede Globo, Kadu Moliterno, foi vítima de um trojan e teve dinheiro da conta corrente desviado. Se quiser assistir a entrevista, baixe do link:

http://www.cursodehacker.com.br/entrevista.zip

Só tem um pequeno detalhe. Os trojans que você está aprendendo a usar neste capítulo são trojans feitos por terceiros. Isso quer dizer que são programas conhecidos, usados por um grande número de pessoas. E são conhecidos também pelos fabricantes de antivírus e antispyware. Ainda não entendeu? Vou ser mais claro: estes trojans são detectados mais facilmente do que o trojan personalizado. A assinatura destes trojans são conhecidas e estão sendo incluídas nos bancos de dados dos antivírus, atualizações do sistema operacional e antispywares. Isto quer dizer que suas chances de sucesso são menores do que se usar um trojan personalizado.

Eu poderia ocultar esta informação e deixar você se decepcionar, já que de cada dez tentativas com trojans, menos de três dão certo. Mas não estou aqui para enganá-lo e sim para mostrar a realidade dos fatos: trojans populares são pouco eficazes.

Trojans Personalizados

O trojan personalizado é aquele feito por você, em Assembly, Delphi, Visual Basic, C++ ou outra linguagem, incluindo a plataforma .Net. Se você não conhece nada de programação, então não tem jeito, vai ter que se contentar com os trojans prontos, que apesar de menos eficazes, também funcionam. Nos links que divulguei neste capítulo você pode acompanhar a atualização dos trojans, aumentando suas chances de sucesso.

Nota: Estou preparando para 2006 um curso de criação de trojans em diversas linguagens, incluindo trojans para celulares e instalados bastando a visita ao site. Cadastre seu e-Mail em nosso site para ser avisado quando este produto estiver disponível.

3º PASSO: Configurar o Módulo Servidor

O módulo servidor, mais conhecido como **SERVER**, é a parte destinada a máquina alvo. Lembra que na história de Tróia os soldados foram escondidos dentro do cavalo? Nosso cavalo de trojan será o **PROGRAMA ISCA** e o *server* representa os soldados que vão abrir as portas do micro e permitir a invasão, como ocorreu com o ataque a cidade de Tróia.

A configuração básica de um server pode incluir:

- como ele será instalado na máquina alvo
- como ele vai notificar ao invasor que o alvo está online
- como ele vai se comunicar com o invasor
- como ele vai se ocultar na máquina alvo
- como ele vai se proteger da remoção
- como ele vai iniciar na máquina alvo

Além de ajustes especiais, como por exemplo inibir os pontos de restauração e o firewall do Windows XP, encerrar processos, interferir na ação do antivírus e do firewall e outros recursos, variando em quantidade e qualidade de um trojan para outro.

Um trojan bastante completo é o Beast, que pode ser visto na figura ao lado:

4º PASSO: Preparar o Módulo Servidor

Depois do módulo server configurado, o hacker começa o preparo para a distribuição. O objetivo desta preparação é tornar o trojan:

- invisível ao antivírus
- atraente a ponto do alvo se interessar em executar o arquivo

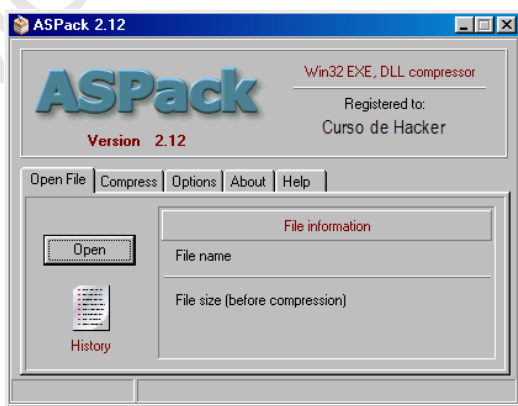
As formas usuais de se conseguir isto são estas:

- compactar e criptografar o server do trojan e/ou o arquivo-isca já preparado
- editar o executável
- juntar o server do trojan a um arquivo-isca

Existem programas conhecidos como compressor de executável. Ao contrário dos compactadores, os compressores reduzem o arquivo sem alterar sua extensão ou funcionamento. Este procedimento serve para alterar a assinatura de trojans e vírus, dificultando a detecção destes arquivos.

O que pode dar errado?

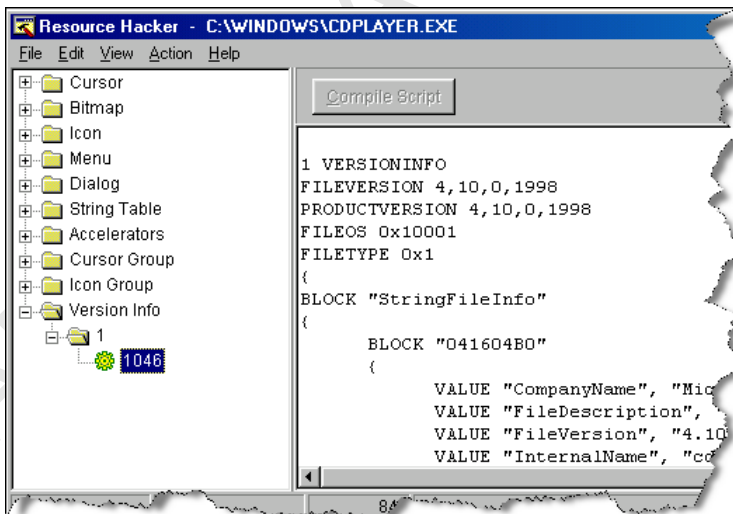
O server do trojan costuma ser um arquivo de alguns poucos kbytes. Alguns destes arquivos podem estar com a máxima compressão possível. Isto significa que o compressor vai exibir uma mensagem de erro ou não vai ter sucesso no processo de compactação. Para contornar este inconveniente, experimente reduzir o arquivo final, com o server já embutido no arquivo-isca. Costuma dar certo.

O petite e o ASPack são dois programas bastante populares nesta função. Veremos como eles funcionam na vídeoaula que acompanha este livro:

O que mais pode dar errado?

Pode ocorrer do antivírus não detectar o trojan depois de comprimido, mas detectá-lo quando o arquivo isca for executado. Isto ocorre por que quando o arquivo é executado, ele é detectado pelo seu *modus operandis* ou por sua assinatura, ao ser descomprimido na memória.

Fazer testes e experimentar taxas de compressão e compressores diferentes, ajuda a vencer mais esta barreira. Também podemos contar com a sorte. Pode ser que o seu antivírus detecte o *server*, mais o do alvo não. isto porque os computadores de quem estuda sobre temas hacker costuma ser melhor protegido do que o do usuário leigo.

Outro tipo de programa que auxilia na preparação do trojan a fim de torná-lo indetectável é o editor de executável. Trata-se de um programa desassemblador, capaz de fazer alterações no arquivo, como alterar o ícone, algumas strings, conteúdo de variáveis, etc...

O Resource Hacker e o PExplorer são dois programas representantes desta categoria:

Nas vídeoaulas que acompanha este livro veremos como usar o PExplorer. melhores resultados no uso deste programa será obtido por quem possui algum conhecimento na área de programação.

Criando o trojan: ocultando o server

Para esconder o server do trojan em um arquivo-isca você vai precisar de um programa do tipo **binder**, também conhecido como **joiner**:

JOIN - Juntar
BIND - Ligação

O que este tipo de programa faz é pegar dois ou mais arquivos e criar um arquivo único, executável. O hacker pega o módulo *server* do trojan devidamente configurado, junta com um arquivo isca e distribui na Internet:

http://www.trojanfrance.com/index.php?dir=Binders/
http://www.un4seen.com/petite/
http://pexplorer.nm.ru/

Não se engane em pensar que é só enviar o trojan, o alvo executar a isca e invadiram felizes para sempre. Na vida real a história é outra. Cada vez mais as pessoas estão se conscientizando dos riscos que correm ao executar arquivos desconhecidos em suas máquinas. Sem falar que o trojan corre o risco de ser interceptado antes de chegar a máquina alvo. Praticamente nenhum dos grandes provedores aceita arquivos executáveis como anexos. Isso significa que o programa-isca deverá de ser zipado antes de ser distribuído. E se ele está zipado, o alvo vai ter que estar muito receptivo para descompactar o programa e executá-lo. Mas apesar da aparente dificuldade, se o hacker convencê-lo de que se trata de um arquivo interessante, as chances de êxito são bem grandes.

5º PASSO: Distribuir o Módulo Servidor para Alvo Certo ou Aleatório

A distribuição do arquivo-isca pode ser individual ou coletiva (spam). Os criminosos que se passam por hackers e usam trojans para roubar senhas de contas bancárias, costumam enviar milhões de e-Mails com iscas. Estas quadrilhas já se especializaram bastante e contam com programadores para criar trojans que são instalados a partir de animações em flash, protetores de tela e cartões virtuais. Alguns se instalam bastando visitar o site que hospeda a página com o código malicioso.

Para criar trojans deste tipo é preciso conhecer mais que o básico de programação, incluindo programação de soquetes.

Além do envio por e-Mail também é possível distribuir o trojan em listas de discussão, no MSN, em salas de bate papo, em sites cadastrados em sistemas de busca e por qualquer outra forma que a imaginação do hacker permitir. No capítulo sobre invasão usando scam veremos formas de distribuição de trojans em massa.

AVISO IMPORTANTE: As pessoas que cuidam da segurança da Internet estão atentas ao envio de spam contendo trojans. Mesmo que a sua intenção não seja desviar dinheiro de contas bancárias, fazer spam com trojan é uma atitude pra lá de suspeita e pode por seu IP na lista negra da Polícia Federal.
Aprenda pelo seu direito ao conhecimento, não se torne um criminoso por tão pouco. Se você é inteligente o suficiente para entender os assuntos que aqui estamos tratando, também é capaz de gerar fontes de renda lícitas. Se precisar de ajuda, conheça meu trabalho a frente do site **http://Prosperidade.Net** e do grupo de discussão no Yahoo! com o mesmo nome.

6º PASSO: Aguardar que o Usuário Execute o Módulo Servidor

Uma vez distribuído o trojan, o hacker precisa aguardar que a vítima esteja conectada a Internet. Nesta fase vamos encontrar duas possibilidades:

1 - O trojan não se comunica com o invasor

Neste caso o hacker vai precisar descobir o IP da vítima. Pode ser lendo o cabeçalho do e-Mail, trocando um arquivo via MSN ou induzindo a vítima a visitar uma página cata IP. Estas técnicas são ensinadas no Curso de Hacker, mas se você não fez o curso, poderá perguntar sobre isto por MSN, e-Mail ou telefone.

2 - O trojan se comunica com o invasor

Os trojans mais recentes, de terceira geração, se comunicam com o invasor toda vez que a vítima estiver online. Estes são os trojans ideais, pois nem sempre dá para saber se a vítima está online e ainda conseguir o IP, tudo na mesma sessão. O hacker fica o máximo de tempo conectado, para coincidir com a hora em que o alvo vai estar online.

7º PASSO: Estabelecer Contato

Para fazer contato com o alvo o hacker usa o módulo cliente. É aquele que

deve ser instalado logo no início, antes mesmo de configurar o server. Se o server foi distribuído com senha, esta senha deve ser informada. Quando o trojan não tem senha, basta alguém com um programa de varredura detectar o trojan, explorar a vulnerablidade antes de você e colocar uma senha para impedir que outros se conectem. Ou seja, você preparou, mais quem vai comer é outro.
O grau de controle sobre a máquina invadida vai depender dos recursos de controle remoto que o trojan oferece e se eles realmente estão disponíveis e funcionando. Alguns trojans apresentam erro em algumas funções (bugs). Há casos em que o uso de certas funções desconectam você da vítima ou desconectam a vítima da Internet. Nesta hora espere de tudo um pouco e mais alguma coisa.

O que fazer quando o trojan funcionar?
Se você chegou até aqui e não tem a menor idéia do que fazer, faltou responder aquelas duas perguntas necessárias em qualquer plano de ataque ou ação hacker:

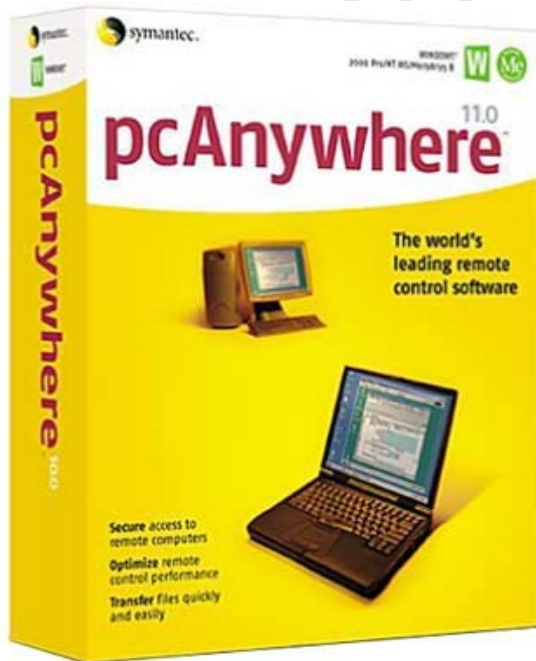
Qual é o alvo?
Qual é o objetivo?

Exemplos de intenções por trás dos trojans
- voyeuirismo ou espionagem
- ativar a webcam e olhar o que se faz naquele ambiente
- capturar arquivos da vítima
- capturar senhas das vítimas
- criar contas de usuário na máquina da vítima
- usar a máquina da vítima como ponte para ataques
- preparar a máquina da vítima para outras técnicas, como DDoS, man in the midle, etc...
- configurar um serviço FTP, P2P ou WWW na máquina da vítima, usando-a como servidor proxy, FTP ou de hospedagem

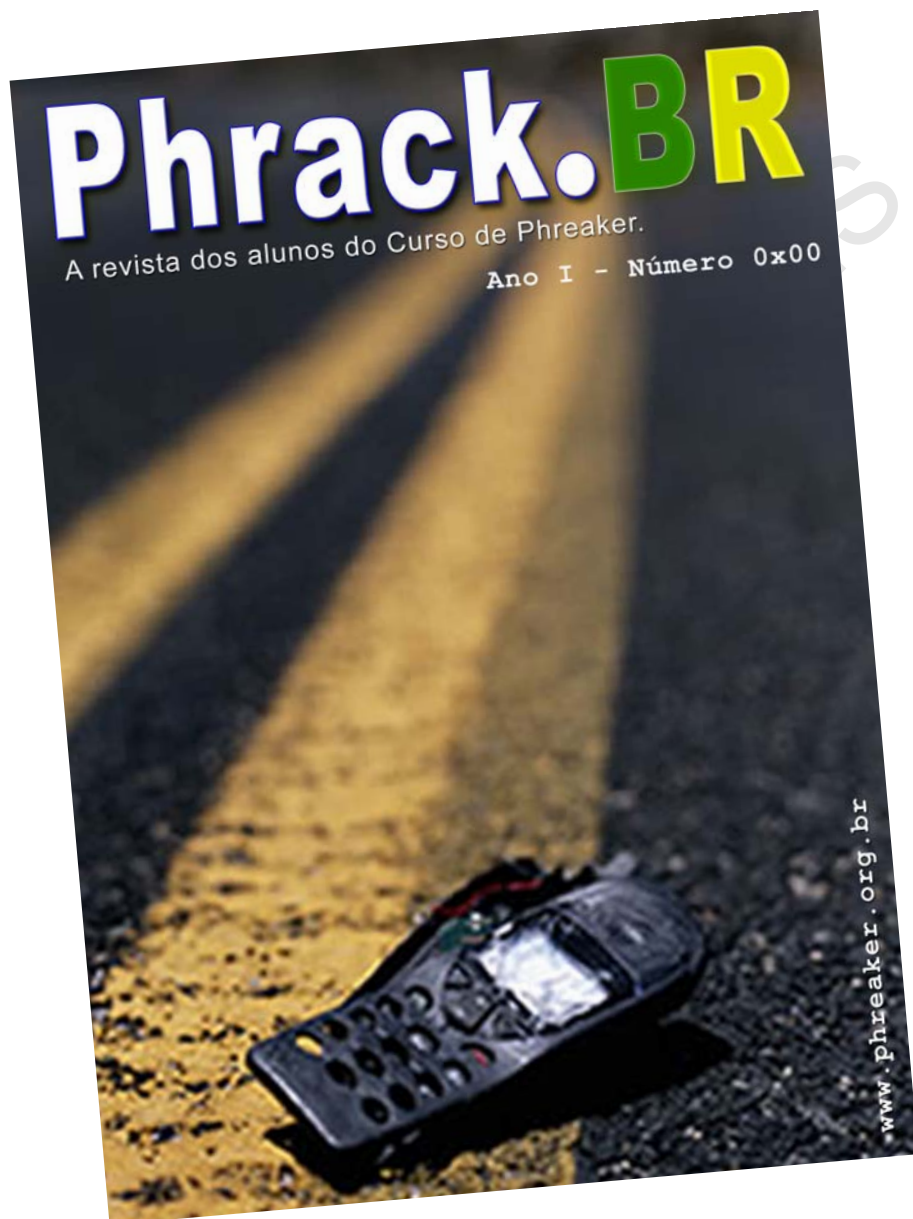
Quando o trojan dá certo o controle é total. Somente o caráter e as intenções limitam as ações.

Um Pouco sobre R.A.T. - Remote Access Tools

Os trojans são programas de computadores da categoria ferramentas de acesso remoto. Programas como o Carbon Copy, PC Anywhere, Assistência Remota, VPN, serviço de terminal e tantos outros, também servem a esta finalidade: controlar um outro micro a distância.
A diferença entre programas como o Back Orificie, NetBus, SubSeven, Beast e outros trojans, é que estes programas são mal vistos. Quando o antivírus os detecta, já sabe se tratar de programas para fins maliciosos.
Programas comerciais como o PC Anywhere, que permite o controle remoto do PC via Internet, são considerados bons programas pelo antivírus. Isto quer dizer que se o hacker usar programas comerciais como trojan, o antivírus não vai reclamar.

http://www.symantec.com.br

Aqui encerra este capítulo. Não esqueça de assistir as vídeoaulas sobre trojans. Elas estão em um dos CDs que você recebeu ao adquirir este livro.

Revista Phrack.BR

www.phreaker.org.br

Capítulo 7:

Invasão com Phishing Scam

Capítulo 7:

Invasão com Phishing Scam

Phishing, Scam, Scammer

Phishing é a combinação das palavras em inglês *password* (senha) e *fishing* (pescando). Scam quer dizer feito por engano. Phishing Scam é enganar o usuário, obter senhas e informações mediante fraude; 'pescaria de senhas'. Quem realiza ações de Phishing Scam é conhecido como Scammer.

Spam

O apresuntado de porco SPAM é fabricado nos EUA pela empresa Hormel desde 1937.

O grupo inglês Monty Python, em um dos episódios de seu programa, exibiu uma cena de bar que a 'proprietária' só tem SPAM no cardápio. No episódio o nome SPAM é repetido à exaustão.

No início da Internet nos EUA, alguém resolveu enviar mensagens publicitárias em massa a vários grupos de discussão. Desde então, as mensagens indesejadas enviadas em grande quantidade são conhecidas como SPAM.

http://www.hormel.com

Spammer

Spammer é quem envia e-Mails não autorizados em grande quantidade. O scammer costuma ser também um spammer, pois é com o envio de mensagens-isca em grande quantidade que o spammer consegue algum resultado. A prática de spam não é proibida e o único caso no Brasil de spammer preso por esta prática, foi por usar o nome de um grande banco nas mensa-

gens. A investigação que resultou na localização do spammer foi uma iniciativa da instituição bancária, que também custeou a operação. O spam é comparado ao envio de mala direta pelo correio. Não há qualquer proibição em fazê-lo. O que vem ocorrendo no Brasil é a autoregulamentação. Os provedores bloqueiam a conta de quem envia spam e domínios suspeitos de SPAM são incluídos em listas negras de programas e servidores.
Isto quer dizer que se você decidir fazer SPAM, poderá ter problemas com o seu provedor e até inutilizar o seu domínio, ao fazer com que ele passe a figurar em listas negras.

O Alvo

Como toda AÇÃO HACKER esta também precisa de um alvo. Os alvos do Scammer tem sido:

• Correntistas de bancos, principalmente os que realizam transações pela Internet.

• Usuários de cartão de crédito.

• Qualquer pessoa que tenha uma conta de e-Mail, principalmente em provedor gratuito.

• Qualquer pessoa que faça compras pela Internet.

• Pessoas e empresas com domínio registrado na Internet.

• Qualquer pessoa que acesse a Internet, pois basta usar uma máquina comprometida para correr riscos.

Alvos que surgiram com as novas tecnologias:

• Qualquer pessoa que acesse uma rede sem fio.

• Usuários de telefones celulares (smartphones) com tecnologia sem fio, como a Bluetooth por exemplo.

Objetivos do Scammer

Objetivo Primário

• Obter a autenticação. Isto quer dizer, reunir as informações necessárias para se fazer passar pela VÍTIMA e obter alguma vantagem financeira.

Objetivos Secundários

• Após obter os dados do cartão de crédito, fazer compras pela Internet.

• Após obter os dados da conta corrente ou poupança, fazer compras

on-line, pagamentos ou transferências.

• Após obter os dados de registro do site, desviar o acesso simulando um defacement.

• Após obter a senha do e-Mail, bloquear o acesso ou acompanhar as mensagens sem que a vítima perceba.

• Após obter a senha do usuário, obter acesso a rede da empresa, servidores, intranet ou extranet.

Peça (A ISCA)

• A PEÇA é o e-Mail ou página ou combinação de ambos e que vai servir como ISCA para atrair o ALVO.

Temas Mais Explorados pelos Scammers

• Receita Federal solicitando recadastramento de CPF ou comunicando alguma irregularidade no imposto de renda.

• Cartões virtuais, às vezes com remetente conhecido.

• Mensagem com anexo, podendo ter extensão DOC, EXE, SCR,PIF, BAT, ZIP, RAR, MP3, XLS. A maioria dos antivírus atuais remove alguns destes anexos, inclusive quando compactados.

• Provedor de e-Mail solicitando a atualização do cadastro.

• Órgão de registro de domínio solicitando senha ou atualização do cadastro.

• Banco ou operadora de cartão de crédito solicitando senha, atualização do cadastro ou pedindo para acessar a página do banco através de link ou imagem no e-Mail.

• Concursos dos mais diversos tipos, principalmente pegando carona em concursos populares como o Big Brother, Casa dos Artistas, Show do Milhão, etc...

• Promoções de lojas virtuais conhecidas, oferecendo produtos com descontos ou preços baixos.

• Companhia aérea com promoção de passagens ou sorteios.

• Fofocas e escândalos envolvendo celebridades, às vezes com anexos ou link para ver fotos ou baixar vídeos.

• Apelo a emoção, enviando link para baixar as ‘provas da traição’.

• Oferta de programas gratuitos, como gerador de crédito para celular, antivírus e correções para o Windows.

• Apelo a curiosidade, quando se comenta um fato curioso e oferece

o link para baixar as fotos ou vídeo.

• Apelo a nostalgia, quando se faz passar por um amigo da escola ou faculdade e quer saber se você é a pessoa com quem se estudou.

• Apelo a ganância, se fazendo passar por algum banco e alegando que foi feito um crédito na sua conta por determinação da justiça, como reparação pelo confisco da poupança ou cobrança de imposto compulsório. No mesmo e-Mail tem o 'link' para acessar a 'conta' no banco.

• Inscrição em reality shows, como o Big Brother Brasil, Show do Milhão, Fama, O Aprendiz, O Grande Perdedor e tantos outros.

• Atualizações de cadastros dos mais diversos tipos.

• Se fazendo passar por alguém conhecido.

• Atraindo a atenção pela linha do ASSUNTO. Em alguns casos basta clicar sobre o e-Mail para comprometer a segurança do micro.

• Avisos de cobrança dos mais diversos tipos.

• Aviso de problema com a documentação da empresa.

• Oportunismo: e-Mails que se aproveitam de qualquer tema da moda ou tragédia. Foi assim na época do atentado de 11 de setembro, na tragédia ocasionada pela Tsunami e nos furacões em Nova Orleans.

• Anexos com animações em powerpoint ou flash: românticas, piadas, espirituais, com remetente conhecido ou não.

• Operadora de telefonia oferecendo identificador de chamada ou celular grátis ou alegando débito em sua conta.

• Oferta de papéis de parede, smiles, protetores de tela, etc...

• Ofertas de acesso gratuito a sites pornográficos ou cassino.

• Aviso de débito em sites de leilão.

• Aviso de ordem de pagamento em aberto.

Por Que Funciona?

As empresas estão melhorando suas estratégias de defesa. Os sistemas operacionais e demais dispositivos de rede estão cada vez mais seguros. Cursos como este e a divulgação de como os hackers agem em livros e sites, faz com que as pessoas se tornem cada vez mais conscientes da necessidade de ter uma ATITUDE DE SEGURANÇA.

A medida que a segurança física e lógica aumenta, as técnicas de invasão passam a contar com a colaboração involuntária da vítima.

Todos os investimentos em segurança bancária são insuficientes para impedir alguém com os dados de acesso - conta, senha, palavra secreta; de

movimentar a conta da vítima.
Técnicas de dissimulação, camuflagem, persuasão, são as novas armas dos invasores. A **ARTE DE ENGANAR**, forma de ataque que tornou Kevin Mitnick famoso e deu nome ao seu primeiro livro, passou a ser conhecida pelo pomposo nome de **ENGENHARIA SOCIAL**.
Ainda funciona por que as pessoas não dispõe de tempo, vontade ou conhecimento para atestar a veracidade de cada e-Mail, cada conexão, cada tela de login. Quem precisa se preocupar em proteger o usuário são as empresas e profissionais da área.
Beira ao sarcasmo sugerir a um leigo que atualize o sistema operacional, escolha entre as centenas de opções do Linux, instale um antivírus, um firewall e um anti-spyware. Que tal incluir também recompilar o kernel?

Pode Piorar?

Pode não, vai piorar. No Brasil somos cerca de 12% conectados. Faltam mais de cem milhões de pessoas ter acesso a Internet. O Governo pretende dobrar este número nos próximos anos, mas o fiasco do PC Conectado leva a crer que a inclusão digital esteja mais certa de ocorrer pelos smartphones e TVs digitais que via micros desktop.
Os milhões de pessoas que ainda não conhecem a Internet vão chegar de repente, a mercê de todo tipo de golpe virtual, dos mais recentes aos mais antigos. Pouca gente se dá conta disso, mas saindo do perímetro das grandes capitais, o Brasil é formado em sua maioria por cidades muito pobres, principalmente na região Norte/Nordeste.
Baixa escolaridade, alta taxa de natalidade e crianças se prostituíndo por um real é cenário bastante comum nestas regiões. Na região Norte e Centro Oeste por exemplo, impera a pistolagem e por cinquenta contos é possível mandar alguém desta para melhor.
A classe média brasileira que mora no eixo Rio-São Paulo, acha que o Brasil é como aparece nas novelas da Rede Globo. Engano puro. Deveriam conhecer a cidade de Breves, no Pará, onde quase 50% das meninas acima de sete anos é prostituída. Será Breves a capital da prostituição infantil? As campanhas que tentam em vão coibir esta prática perniciosa tem se concentrado nas cidades turísticas do litoral. A impressão é que a pedofilia é autorizada dentro de casa, só não pode sexo com estrangeiros.
Se este é o Brasil real, não resta dúvida que este Brasil de miseráveis e semi-analfabetos está a mercê de pessoas maliciosas que encontram na

tecnologia formas de aplicar novos e antigos golpes.
Também não devemos esquecer das tecnologias emergentes como Bluetooth, Wi-fi, VoIP, os celulares inteligentes (smartphones) a o rádio e TV digital. Vai ser suficiente estar caminhando pelas ruas da cidade para ter seu celular invadido e seus dados roubados. Aquele rapaz sentado à mesa do McDonald's com o notebook talvez esteja agora mesmo acessando a rede de alguma empresa.
A cada dia surgem novos termos para dar conta da segmentação do setor de invasões. É conhecido como **Wi-phishing** a técnica de scam em redes sem fio. Outro exemplo é o envenenamento de DNS, uma técnica nem tão recente , que ganhou roupagem nova com o nome **Pharming**. O pharming consiste em alterar a tabela de DNS de um ou mais servidores, fazendo com que toda requisição de página, como por exemplo www.banco.com.br, seja desviada para um endereço controlado pelo scammer. Se a página falsa for uma cópia fiel da página verdadeira, é possível que até profissionais experientes sejam vítimas deste golpe.

Como Se Proteger

A orientação para o usuário se proteger de ataques do tipo Phishing Scam é:

• Só abrir anexos de e-Mail vindos de pessoas conhecidas, nos casos de extrema necessidade e que você tenha conhecimento prévio do que se trata.

• Restringir a visitação a sites conhecidos, algo difícil de ser conseguido na prática, devido a curiosidade natural das pessoas.

• Suspeitar de qualquer alteração na autenticação da rede ou dos serviços bancários.

• Nunca fornecer os dados do cartão de crédito na Internet. O que também é muito difícil de manter, pois existem boas ofertas de compras na Internet. Mas pelo menos limitar o uso do cartão às empresas renomadas, como Submarino, Americanas, Saraiva e outras deste porte.

• Lembrar que a Receita Federal, Serasa e rede bancária NUNCA pedem senhas por e-Mail.

• Nunca clicar em links de e-Mail. Prefira digitar o endereço na barra do navegador.

• Ter muita atenção ao digitar o endereço dos sites de bancos, pois podem se aproveitar de erros de digitação e desviar sua conexão. Esta

técnica é conhecida como typosquatting.

• Nunca digitar senhas em **micros promíscuos**, aqueles que todo mundo usa.

• E por último aquele blá blá blá que a gente conhece: sistema operacional atualizado, instalar antivírus, firewall e anti-trojan, manter tudo atualizado, recompilar kernel,... ;)

• Uma dica simples que costuma funcionar é digitar a senha errada de propósito da primeira vez. Se for uma peça de phishing scam, após a primeira digitação você vai ser direcionado a página verdadeira. Mas não conte muito com isso.

Phishing passo-a-passo

1º PASSO: Definir o ALVO
2º PASSO: Definir o OBJETIVO
3º PASSO: Clonar ou elaborar a PEÇA (isca)
4º PASSO: Criar a BASE DE DADOS
5º PASSO: Definir a ESTRATÉGIA
6º PASSO: Enviar e-Mail em massa (SPAM)
7º PASSO: Receber e Analisar o Retorno
8º PASSO: Ação Hacker

1º PASSO: Definindo o ALVO

A primeira decisão do scammer é decidir a quem pretende atingir com esta ação hacker. Já vimos no início deste capítulo uma lista de alvos em potencial.

2º PASSO: Definindo o OBJETIVO

Após a definição do ALVO o scammer define qual será o objetivo desta ação hacker. Já vimos que existe um objetivo PRIMÁRIO e outro SECUNDÁRIO. É pela definição do OBJETIVO que o scammer irá determinar qual será a melhor estratégia para o seu PLANO DE ATAQUE.

3º PASSO: Clonar ou Elaborar PEÇA (a isca)

A peça do scam ou a isca se preferir, tanto pode ser uma criação do scammer, como uma cópia de campanha real.

A maior parte das peças de scam que você vai se deparar tem erros grosseiros de ortografia e gramática. A composição também não é das melhores e

os links são os mais ridículos possíveis, assim como as tentativas de mascaramento.
Mas apesar de toda esta imperfeição, o número de vítimas não para de crescer. Programas do tipo Web Crawler capturam todo o comteúdo do site, facilitando bastante na hora da clonagem ou da adaptação de uma peça aos interesses do scammer.

4º PASSO: Criando a BASE DE DADOS

O próximo passo do scammer é a criação de uma base de dados ou lista de e-Mail (mailing list). Quem tiver o seu nome em uma lista de scammer, de tempos em tempos será contemplado com iscas. Mesmo aqueles que possuem conhecimento suficiente para não cair neste tipo de golpe, no mínimo serão importunados com as mensagens indesejadas (spam).

A base de dados pode ser obtida de várias maneiras:

- Compra.
- Capturada via Google.
- Capturada por um Web Crawler usado contra páginas da Internet, salas de bate papo, fóruns, etc...
- Extraída dos arquivos do Outlook Express.
- Capturada em listas de discussão.
- Criada a partir da combinação de nomes próprios, palavras e combinações de caracteres + o sufixo dos provedores de e-Mail.

5º PASSO: Definir ESTRATÉGIA

Estas são algumas das estratégias do scammer:

- Clonar campanha publicitária legítima que esteja em andamento.
- Se aproveitar de algum fato extraordinário, como os já citados atentado de 11 de setembro, Tsunami e falecimento do Papa João Paulo II.
- Typosquatting - registro de domínio com grafia quase idêntica ao original. O usuário, ao digitar o endereço com erro de digitação, vai abrir o site clonado sem que perceba. Esta técnica, quando bem elaborada, pode enganar até um profissional experiente.
- Envenenamento de cache (DNS Cache Poisoning).
- Cross Site Scripting.
- Engenharia social.
- Trashing.
- Spyware.

6º PASSO: Enviando e-Mail em Massa (SPAM)

O scammer experiente vai ter cuidado nesta etapa, pois é uma das mais críticas e é quando poderá ser preso em flagrante. Para enviar e-Mail em massa o scammer vai precisar de um serviço SMTP que pode ser o de uma conta de e-Mail gratuito. Uma outra opção é usar SMTP próprio em Windows ou Linux.

Scammers descuidados enviam a massa de e-Mails de suas conexões domésticas, tornando-se alvo fácil para uma prisão em flagrante. A forma menos arriscada de enviar o spam com a isca é através de um micro promíscuo, como os dos cybercafés, por exemplo.

No Brasil já temos pelo menos um caso de prisão em flagrante de scammer. Ocorreu no Piauí, no momento do envio dos e-Mails. Provavelmente o scammer manteve atividades frequentes naquele local, dando tempo da Polícia Federal localizá-lo e obter o flagrante.

A quantidade de e-Mails que pode ser enviada por hora depende da conexão, do sistema operacional, da rede e do programa de envio. Outro deslize cometido pelo scammer iniciante é consultar o e-Mail de retorno de uma conexão rastreável.

O que é o e-Mail de Retorno?

É o e-Mail que vai receber as mensagens contendo informações das vítimas. Se o scammer optar por hospedar um banco de dados junto com a página clonada, corre o risco de não conseguir recuperá-lo, pois os sites de scammers são fechados rapidamente.

O e-Mail de retorno ideal é aquele criado em provedor no exterior e que usa redirecionamento em cascata passando por várias contas. Este procedimento torna praticamente impossível chegar ao destinatário das mensagens com a brevidade necessária.

Outra solução adotada pelos scammers para dificultar o rastreamento é enviar as mensagens para um aparelho celular, que pode ser comprado sem registro nos classificados e oficinas de manutenção. Espero que esta informação sirva de alerta caso algum dia você se desfaça do seu celular.

7º PASSO: Receber e Analisar o Retorno

O scammer inexperiente poderá se comprometer nesta etapa se o e-Mail de retorno for acessado a partir de uma máquina qualificada. Um scammer experiente vai acessar a conta de e-Mail de um micro promíscuo e em

hipótese alguma vai fazer qualquer outra operação que o identifique na mesma sessão.
A medida que for recebendo as informações de retorno por e-Mail, o scammer poderá dar início a uma série de ataques e vender ou distribuir estas informações para dificultar as investigações. Se você freqüenta os canais underground do IRC já deve ter se deparado com ofertas do tipo.
Quando os primeiros e-Mails começarem a chegar para os usuários, alguém vai dar o alerta e é provável que em poucas horas, no máximo dias, o site esteja fechado.
Com os dados do retorno em mãos o scammer parte para a AÇÃO HACKER prevista no PLANO DE ATAQUE.

8º PASSO: Ação Hacker

Os scammers presos, costumam ser enquadrados nos crimes de estelionato, lavagem de dinheiro, quebra de sigilo bancário sem autorização judicial, formação de quadrilha, entre outros.
Se passou pela sua cabeça contar com a falta de lei específica contra crimes de informática, perceba na relação acima que o Código Penal é mais que suficiente para causar a condenação do scammer.
Os cúmplices do scammer, pessoas que cedem suas contas bancárias ou quitam suas contas através de meios fraudulentos, são conhecidos como LARANJAS e punidos nos rigores da Lei.
A julgar pelo que é publicado na imprensa e pela quantidade de peças de scam que circula pela Internet, concluímos que grupos de fraudadores já descobriram este nicho de mercado e estão investindo tempo e dinheiro nesta prática criminosa.

Consequências Para o Scammer

No Brasil já existem vários casos de prisão pela prática do phishing scam. A polícia está cada vez mais preparada para lidar com este tipo de crime. E mesmo que não esteja explícito em nosso Código Penal, ele pode ser tipificado em outros artigos.
Percebo no IRC que alguns jovens acreditam sinceramente que não serão pegos. Alguns adultos também costumam me perguntar se terão problemas se usarem cartões de crédito e informações de contas bancárias roubados pela Internet.
Mesmo que você tome todos os cuidados para evitar rastreamento ou ob-

tenção de provas contra você, contamos com seu bom senso para não se tornar um criminoso. Não é por que é fácil que deve ser feito. Use este conhecimento para a sua proteção e a proteção de seus contratantes, amigos e familiares. Será que é isto mesmo que você deseja? Uma vida de crimes?

Consequências Para o Usuário

Os usuários vítimas de scam passam por uma verdadeira *Via Crucis* até conseguir ressarcimento, isto quando ele ocorre. O ator Kadu Moliterno da TV Globo foi vítima de um scam em abril de 2005. Por causa deste incidente fui convidado a participar do programa Sem Censura da TV Educativa/TV Cultura, levado ao ar no dia 11 de maio de 2005. Na ocasião procurei deixar claro que o ator teve seu caso resolvido em menos de 24h por ser uma pessoa pública e funcionário do principal veículo de comunicação do país. Pelos relatos de muitos de nossos alunos este ressarcimento a jato não é a regra.

O principal problema do usuário é provar que não é ele mesmo que está tentando aplicar um golpe no banco. A responsabilidade pelo uso da senha é do usuário e o banco não é obrigado a ressarci-lo se a conta foi acessada com a senha. O problema aqui é saber se o cliente não deu a senha a alguém propositalmente. O sistema é passível de fraude e o usuário típico não tem capacidade para detectar anomalias no sistema de autenticação.

Consequências Para a Empresa

O prejuízo das empresas vítimas de scam não é só financeiro. Inclui a perda de credibilidade e até a desvalorização da marca. Um site de cartões virtuais por exemplo, pode vir a fechar as portas se chegar ao ponto de ninguém mais confiar nos seus serviços.

Na parte financeira, se o cliente conseguir provar que não foi o responsável pela compra ou retirada do dinheiro da conta, a empresa terá que ressarci-lo e talvez indenizá-lo. Não concordamos com o cenário atual, onde as empresas e profissionais de TI não são punidos, apesar da notória incompetência para coibir este tipo de golpe.

Os usuários continuam expostos e os hackers são usados como bodes expiatórios. Mas nem são os hackers a causa do problema e nem os clientes estão em condição de se proteger.

Conclusão

A abolição da prática do scam só será possível através de uma ação conjunta envolvendo os veículos de comunicação, os hackers do bem, o Governo Federal, o Congresso Nacional, empresários, profissionais de TI, desenvolvedores, instituições de pesquisa, ONGs e fabricantes de software. As empresas e profissionais de TI também precisam ser responsabilizados pelos prejuízos causados por seus serviços e produtos que não oferecem segurança.

Ao apresentar o hacker como a causa do problema, o que estas pessoas fazem é varrer a sujeira para debaixo do tapete. Não são os hackers que criam sistemas operacionais ou que administram as redes das empresas invadidas. A falha está lá, criada pelo fabricante do produto ou mantida pelo profissional de TI. O hacker é um agente oportunista. Nunca deve ser visto como o criador do problema. Ele está bem longe de ser a causa, embora possa ajudar na solução.

Advertência (mais uma)

O objetivo deste capítulo e das vídeoaulas no CD é demonstrar como os hackers usam o scam para obter senhas de usuários. Use esta informação para proteger a si próprio, seus clientes e amigos de ataques e invasões.

Em momento algum sugerimos que este conhecimento seja usado contra terceiros e caso isto tenha ocorrido, favor desconsiderar a informação e nos comunicar para que possamos readequar o texto das futuras edições.

Todas as práticas aqui descritas foram testadas em nossa rede interna ou IP sob o nosso domínio no momento da demonstração. Não nos responsabilizamos caso você venha a fazer mal uso destas técnicas.

Invadir uma conta bancária corresponde a quebra de sigilo bancário sem autorização, o que é um crime previsto em Lei. Lembre-se: com o conhecimento vem a responsabilidade.

Capítulo 8:

Invasão de e-Mail

Capítulo 8:

Invasão de e-Mail

O objetivo deste módulo é esclarecer de uma vez por todas os fatos por trás da invasão de contas de e-Mail. Gostaria de começar apelando para o seu bom senso: se a invasão de e-Mail fosse algo possível de ser feito em 100% dos casos, como ficaria a segurança das pessoas? Se fosse algo possível de ser feito em 100% dos casos, você não acha que as minhas contas de e-Mail já não teriam sido invadidas? Ou a do presidente da república?
Antes de seu desânimo completo, quero dizer que é possível invadir contas de e-Mail, mas não com a facilidade ou índice de sucesso próximo a 100% como alguns querem nos fazer pensar.
E não estou falando de sistemas seguros. De nada adianta o provedor ser uma fortaleza se o usuário comete ato falho, que permita a descoberta da senha do e-Mail.
Cada invasor tem um percentual diferenciado de sucesso na descoberta de senhas de e-Mail. Isto inclui um pouco de sorte. Invadir uma conta de e-Mail exige que se tenha alguma estratégia. Envolve o uso de técnicas combinadas. Ás vezes damos sorte e descobrimos a senha logo de cara. Mas as senhas melhor elaboradas podem representar um desafio mesmo para os hackers mais experientes. Este processo é amarrado pelo raciocínio, pelo ‘modo de pensar hacker’.
Lembro bem de um aluno que não conseguia de forma alguma localizar sites vulneráveis para ver o funciomaneto das invasões sem ferramentas. Se escondendo atrás da incompetência, chegou a culpar o curso por não conseguir localizar tais sites. Em uma sessão de *chat* procurei e na mesma hora localizei três sites vulneráveis, explicando o processo de raciocínio envolvendo cada uma das buscas. Adiantou? Nada. O aluno continuou na mesma, sem a capacidade de localizar os sites vulneráveis. Por mas que eu queira, não posso resolver problemas de má formação acadêmica ou preguiça mental. Foge completamente ao nosso objetivo e capacidade.

Alguns leitores ou alunos do curso, o máximo que vão conseguir é reproduzir nossos exemplos e exercícios. Principalmente no que diz respeito a este capítulo. Tenho e-Mails e mensagens em nossa lista de discussão, de alunos do curso gratuito, que desde as primeiras lições entendem como a coisa funciona e conseguem descobrir senhas de e-Mail pela dedução.
E também tenho algumas mensagens de alunos já no final do curso, que se limitaram a **colecionar o material de estudo**, aguardando uma oportunidade para colocar tudo em prática. Talvez tenham esquecido que este conhecimento hacker é bastante volátil. O que eu ensinei a um ano atrás, hoje pode não servir para muita coisa. Se em 2003 eu falava em NetBus nas aulas de trojan, para 2006 eu sugiro que se crie trojans personalizados, incluindo variações para telefones celulares. É um conhecimento que se perde se não for colocado em prática.
Só para lembrar: toda esta conversa é para dizer que o sucesso das suas intervenções em e-Mails depende mais de você do que das técnicas que vamos ensinar. Depende de você pensar da maneira certa. De saber combinar as técnicas. De você praticar bastante para ir aparando as arestas e assimilar as diferenças entre os diversos sistemas de proteção.
Atualmente eu posso dizer que consigo resolver a senha de mais de 90% das solicitações. Mas este é um serviço pelo qual eu cobro. Além disso eu exigo a assinatura de um termo de responsabilidade, onde o solicitante declara que o e-Mail a ter a senha revelada é próprio e me isenta de qualquer responsabilidade.
É mais ou menos como o chaveiro que é chamado para abrir uma fechadura. Ele precisa de alguma garantia de que o solicitante é pessoa idônea.
A idéia inicial ao oferecer este serviço foi devolver aos legítimos donos, suas contas de usuário roubadas por hackers. Curiosamente a maior parte dos pedidos de quebra de senha de e-Mail vem de pessoas de ambos os sexos que se sentem traídas pelo(a) companheiro(a). Cá pra nós, quando pinta a desconfiança, é sinal que alguma coisa já rola faz tempo. Não precisa olhar o e-Mail para descobrir isso.
Invadir uma conta de e-Mail sem autorização é crime comparado a quebra de sigilo da correspondência. Embora a detenção não se aplique neste caso, prepare-se para pagar algumas cestas básicas ou até mesmo meia-geladeira, que é a sentença mais comum nestes tempos de superlotação dos presídios.

Decepção ao abrir a caixa postal

Os relatos de quem invade uma conta de e-Mail e também de quem contrata uma invasão, geralmente é de decepção. O problema aqui é deixar a imaginação fluir. Alguém em busca da prova da traição espera encontrar e-Mails marcando encontros, fotos comprometedoras, talvez vídeos e MP3s com gemidos e susurros. Se eu for me ligar no que diz a psicologia, vou acabar acreditando que o traído sente prazer em saber da fornicação do outro. Jung a parte, a decepção ocorre justamente por que:

- as mensagens não trazem as revelações esperadas
- as mensagens foram baixadas do servidor por algum cliente de e-Mail, como o Outlook por exemplo. Então o acesso pelo Webmail revela uma caixa de entrada vazia ou com quase nada

Independente dos seus motivos ao querer descobrir senhas ser de cunho sexual ou não, esteja pronto para estas decepções: não encontrar as mensagens que esperava ou não encontrar mensagem alguma, por terem sido baixadas para o micro do usuário.
Agora que você foi imunizado(a) podemos passar a descrever as técnicas, voltando a lembrar que o sucesso aumenta quando as técnicas são combinadas entre si e amarradas com o modo de pensar hacker.
E só para lembrar, é crime invadir contas de e-Mail, comparado a quebra de sigilo da correspondência.

Descobrindo Senhas de e-Mail

TÉCNICA 1: Dedução pura e simples. Elementar meu caro Watson

Uma das técnicas mais subestimadas e que costuma apresentar elevado índice de acertos é a dedução. Gostaria de comentar um fato ocorrido em uma palestra para profissionais de TI altamente gabaritados. Quando eu comentei ser esta uma técnica poderosa, começou um rumorejo seguido de risinhos de deboche. Foi quando percebi que o grupo estava confundindo dedução com advinhação. Não é preciso dizer que o tal risinho passou pra mim e eu tive que tossir um pouco e beber água pra disfarçar. É notório que profissionais de TI gabaritados deixam a desejar no quesito cultura. Mas eu ainda me surpreendo.
Para que você não cometa o mesmo erro que seus futuros colegas (?) vamos definir cada palavra:

ADIVINHAR
[Do lat. addivinare < lat. ad divinare.]
Verbo transitivo direto.
1.Conhecer ou descobrir, por meios sobrenaturais ou artifícios hábeis, o que está oculto em (o passado, presente ou futuro).

DEDUZIR
[Do lat. deducere.]
Verbo transitivo direto.
1.Tirar de fatos ou princípios; tirar como conseqüência; inferir, concluir:
2.Tirar como conseqüência lógica; inferir, concluir.

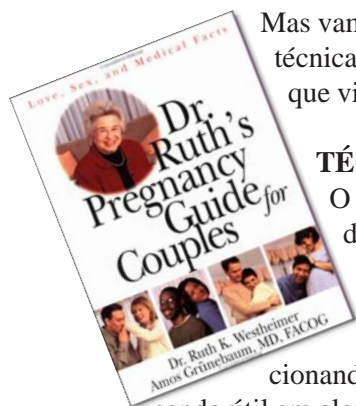
Fonte: Novo Dicionário Eletrônico Aurélio versão 5.0

Quando eu sugiro o uso da DEDUÇÃO como técnica de quebra de senha de e-Mail, estou me referindo a capacidade que temos de tirar conclusões. Nada a ver com esoterismo, exoterismo ou o que o parta. Então DEDUZIR não é ADIVINHAR.
Para aguçar a sua capacidade de dedução, sugiro que antes de experimentar técnicas mais elaboradas, tente como senha de e-Mail (ou conta de usuário) cada uma das opções de senha a seguir:

1. Em branco
2. Igual ao nome de usuário
3. Abreviatura do nome do usuário
4. Iniciais do nome de usuário
5. Sequencias de números, como **123456** por exemplo
6. Um único algarismo, como **111111** por exemplo
7. Sequências do teclado numérico, em qualquer direção
8. Sequências de letras do alfabeto, como **abcdef** por exemplo
9. Data de nascimento do usuário ou de alguém próximo
10. Apelido de infância
11. O nome de uma cor
12. Um signo do zodíaco
13. Palavras cristãs, como **jesus**, **deus**, **aleluia**, etc...

14. O CEP da residência ou da empresa
15. O CEP com o zero substituído pela letra **O** ou pelo **@** (arroba)
16. Número do telefone fixo ou celular
17. Placa do carro
18. Nome de filhos, conjuge, pais ou parentes
19. Nome do animal de estimação
20. O sobrenome do usuário
21. Senha numérica curta, com até quatro casas
22. Senha antiga
23. Senha igual a de algum outro serviço, mais fácil de ser invadido
24. Senha padrão do programa, configurada pelo fabricante ou fornecida pelo provedor
25. Número de documento, como RG, CPF, passaporte, etc..., no todo ou em parte
26. O ano em que estamos
27. Uma palavra obscena
28. Nome da empresa
29. Palavra relacionada ao ambiente de trabalho ou hobby
30. Combinações óbvias como por exemplo **marco2006**

Fonte: “Proteção e Segurança na Internet”, 1ª Edição, 2002. Marco Aurélio Thompson, Editora Érica, pág. 57-62

Quando se trata de usuário leigo, as chances de acerto beiram a 70%. Quando a conta é de um usuário experiente, quem sabe um hacker, as chances com o método acima diminuem exponencialmente. Mas não deixe de começar por este processo de dedução e tentativa e erro. Veja se a sua própria senha não se encaixa em uma das opções acima.
Por causa de uma senha fraca, o hacker mais famoso do mundo, Kevin Mitnick, teve seu site pessoal invadido poucos dias após sair da prisão. Entre os alunos do curso é comum aparecer gente desesperada por ter perdido sua conta de e-Mail. Ao saber que pela dedução todas aquelas possibilidades seriam tentadas, deveria ser suficiente para mudarem de senha. Infelizmente nem sempre é assim. É mais ou menos o que ocorre com o HIV. As pessoas sabem do problema, mas pouquíssima gente tem usado preservativo durante as fornicações. Ou vocês acham que o Mick Jagger queira ter filho com a Luciana Gimenez? Só as meretrizes tem conseguido dos homens o uso do preservativo durante cópula.

Mas vamos deixar a Drª Ruth de lado e conhecer mais técnicas de invasão de contas de e-Mail. Foi pra isso que viemos.

TÉCNICA 2: Com força, bruto

O método da força bruta (brute force), se direcionado a contas remotas, é pura perda de tempo.

Se você não conhece esta técnica, vou descrevê-la em detalhes, pois mesmo não funcionando para senhas de e-Mail remotas, ela continua sendo útil em alguns casos de quebra de senhas local.

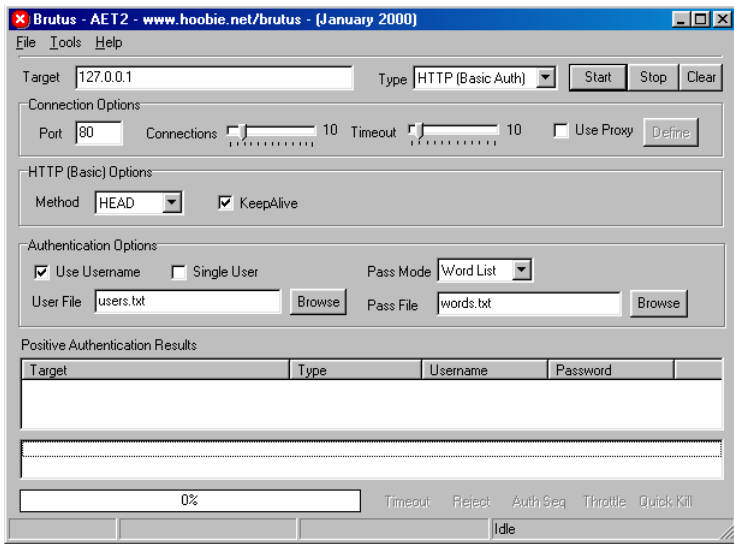
O método da força bruta consiste na tentativa e erro. É diferente da tentativa e erro que você vai fazer com o método da dedução. Quando se trata da técnica da força bruta, estamos falando de milhares de tentativas por minuto. O primeiro problema desta técnica na quebra de senhas de e-Mail é que as milhares de tentativas serão algo do tipo:

```
hhuytg
akirds
cvgfrt
kytfv4
easw4r
rbvg65
```

Você acha que alguém usa senha deste tipo? Nem eu. Então o primeiro problema desta técnica é que as milhares ou milhões de combinações podem passar longe da verdadeira senha.

O programa mais comum para quebra de senhas de e-Mail por força bruta é o Brutus, que pode ser baixado de www.hoobie.net/brutus/brutus-download.html.

O problema das senhas geradas a moda 'vamôsimbora' é a frustração de ver milhões de combinações não funcionarem. Para resolver isto, os programas de força bruta - inclusive o Brutus - aceitam listas de palavras externas, com três opções de uso:

1. Uma lista de palavras a serem tentadas como a senha do usuário.

Neste caso o nome do usuário é conhecido e só a senha é que vai variar.

2. Duas listas, sendo uma de nomes de usuário e outra de senhas. Útil quando não temos o nome do usuário ou quando vamos buscar senhas de vários usuários.

3. Uma combinação das palavras da lista com outros caracteres. A maior utilidade desta opção é poder combinar automaticamente o nome do usuário com números:

lesbao1965
lesbao2003
lesbao40
lesbao300000

E a pergunta é: onde conseguir estas listas de palavras?

No mundo hacker, listas de palavras são conhecidas como dicionários ou *worldlists*. Elas podem ser baixadas prontas da Internet ou criadas por você. Vejamos os dois casos.

Baixar as listas da Internet

O problema das listas baixadas da Internet é um só: no Brasil não tem listas para baixar da Internet. Infelizmente nossa cultura não inclui cooperação. É cada um por si e o governo por todos, sustentando os miseráveis

com cestas basicas, vale gás e o mais que o valha para manter quieta a população. Então não espere cooperação dos hackers brasileiros. Não espere sites com downloads de programas hacker nacionais (existem ?), listas de senhas, tutoriais decentes. Entre em um canal do IRC e diga que quer aprender a ser hacker. Além de ser xingado, ter que ouvir (ler) um monte de baboseira de quem não sabe o que diz, ainda corre o risco de ser banido ou invadido minutos depois.

Analise o teor das listas de discussão hackers e as conversas giram em torno de 'o meu é maior que o seu','vou te quebrar', além de pedidos pra lá de pessoais, que em nada contribuem para a cultura hacker no Brasil.

O título de 'melhores do mundo' parece ter subido a cabeça deste pessoal, pois continuam fazendo defacements em sites pra lá de capengas.

Cadê as invasões a portais do porte do Globo.Com? Receita Federal? Pelo menos uma página de banco pichada? Viu alguma? Nem eu. Que tal invadir o site www.cursodehacker.com.br, online desde quando inaugurado?

Não sei quem está medindo esta capacidade do hacker brasileiro, mas parece que estão puxando a trena pro lado errado.

O hacker brasileiro é o mais baderneiro do mundo e o menos colaborador.

Durante um tempo saí em busca de grupos organizados e o que encontrei foi grupos de duas ou três pessoas, sem nada de especial para ofercer à comunidade, a não ser um punhado de scripts prontos para uso.

Apesar de terem sido contatos online, pude perceber que os hackers americanos, europeus, russos e argentinos são muito mais coolaboradores que nós brasileiros. Até o aumento de oferta de arquivos nas redes P2P só está ocorrendo no Brsil por que quem não dá, não come.

Um país com os melhores hackers do mundo e não existe eventos hacker? Por que será? É porque metade não vai para não dar Ibope ao organizador e a outra metade não vai para falar mal depois. Sinto saudades da Defcon e da Black Hat. Espero que a ABSI consiga mudar isto a longo prazo. Nem que seja de forma compulsória, como fizemos com o banco de tutoriais, onde para ter acesso é necessário contribuir com um tutorial próprio.

Voltando ao tema de como obter listas de palavras nacionais, o que você pode fazer é buscar por listas em outro idioma, como o inglês, passá-las por algum tradutor, como o Power Translator e ter assim a sua lista de senhas. Neste link tem algumas boas listas que você poderá baixar: http://www.hackemate.com.ar/wordlists/. Tem até um dicionário com 2GB, alem de outros menores, temáticos.

Listas Criadas por Você

Outra opção é você mesmo criar suas listas para ataques por força bruta. A primeira opção é digitar palavra por palavra no bloco de notas ou outro editor de texto puro. Sob certa ótica, uma pequena lista com as palavras relacionadas ao ambiente do alvo pode ser mais eficaz que uma lista com palavras a granel.

Uma opção mais viável é usar algum programa gerador de listas. São programas que lêem arquivos texto e separam palavra por palavra, eliminando as repetidas. Você pode salvar páginas com listas de times, com signos, com nomes de bebês, baixar e converter em TXT livros digitais e se fizer direito, em pouco tempo terá um dicionário com milhares de palavras em língua portuguesa.

Mas...

```
[Do lat. magis.]
Conjunção.
1.Exprime oposição ou restrição; porém, todavia,
entretanto, no entanto, contudo.
```

Fonte: Novo Dicionário Eletrônico Aurélio versão 5.0

O legal da conjunção *mas* é que ela põe em cheque tudo o que você diz antes. Esperimente falar assim com a sua esposa: _"Você está linda, mas...". O nosso *mas* no contexto da quebra de senhas foi para preparar o terreno para a péssima notícia que tenho que dar: mesmo que você tenha uma excelente lista de palavras, todos os principais serviços de e-Mail atuais tem proteção contra ataques por força bruta. Já na terceira tentativa o provedor vai bloquear o acesso à conta, de forma temporária ou definitiva. Quer dizer que de nada adiantou o Brutus fazer milhares de tentativas por minuto? Isto mesmo. De nada adianta este potencial de fazer milhares de tentativas por minuto, se já na terceira o provedor bloqueia o acesso. E dependendo do sistema de segurança que o provedor utiliza, o Brutus poderá continuar recebendo *feedback* e apresentar uma senha que nada tem a ver com a verdadeira. Ou então, depois de horas de espera, retornar a mensagem *not found*. Acho que agora você entende o motivo de suas experiências com o Brutus não terem dado certo. A força bruta na invasão de e-Mails deixou de funcionar faz tempo. E não é só com o Brutus, outros programas similares também não funcionam mais.

Porém...

```
[Do lat. proinde, 'por conseguinte', pelo arc.
porende, 'por isso', com apócope.]
Conjunção.
1.Contudo; mas; todavia.
```

Fonte: Novo Dicionário Eletrônico Aurélio versão 5.0

O *porém* é da mesma laia do *mas*. Também serve para reverter uma afirmação e como a primeira afirmação já foi revertida, esta segunda reversão faz aparecer uma luz no fim do túnel. Será que vamos conseguir revelar o segredo por trás das senhas de e-Mail?
Vamos sim, mas deixei isso para a vídeoaula que está no CD, senão perde a graça. ☺

Capítulo 9:

Invadindo o Próprio Micro

Capítulo 9:

Invadindo o Próprio Micro

Se você é daquelas pessoas sensíveis, que não consegue assistir a uma retossigmoidoscopia sem fazer careta, deve estar torcendo o nariz para o título deste capítulo. Afinal, tudo o que você não quer é ter seu micro invadido. Ainda mais agora, depois de saber tanto sobre o assunto e já se achar um hacker. Não julgue pelas aparências. Isto é preconceito. O objetivo de você invadir o seu próprio micro é que, ao invadi-lo você poderá ver onde estão as vulnerabilidades. Você precisa fazer isto antes que outra pessoa encontre as falhas, pois provavelmente não terão a mesma intenção que você.

Como se invade o próprio micro?

O processo de invasão do próprio micro é muito próximo ao processo de invasão do micro alheio. O diferencial é que você tem muito mais informações a seu próprio respeito e poderá ir direto ao ponto. Usando como exemplo a identificação do seu sistema operacional, você poderá ir na seção de exploits do site http://packetstormsecurity.org/ e ver se encontra algum que se aproveita da sua plataforma. A propósito, a coleção **Invasão.BR** é formada por três volumes. Espero que você tenha gostado deste primeiro a ponto de se interessar também pelos outros dois. Sobre a invasão com exploits eu explico já no segundo volume.

Mas como eu ía dizendo, ter informações sobre o sistema poupa tempo e dá para fazer testes específicos e busca de vulnerabilidades especificas. Estes testes de intrusão autorizados são conhecidos no mercado de TI como testes de penetração ou pen(etration) test. Geralmente no Brasil, hackers não fazem pen test. Isso é função do pessoal de TI.

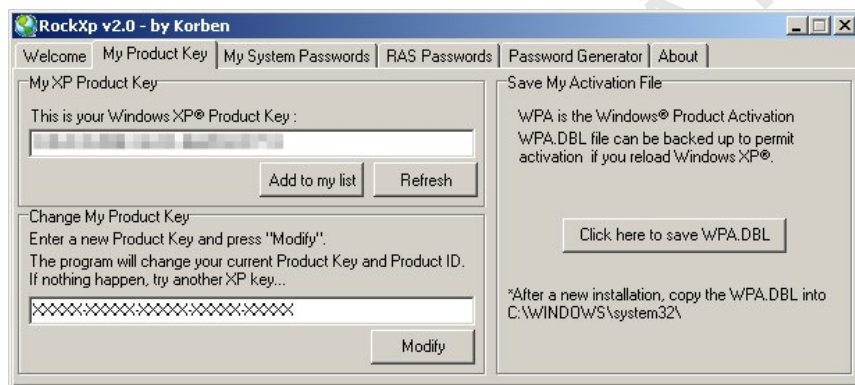
As formas de fazer o pen test em sua própria máquina são estas:

- coleta local
- varredura usando loopback

- varredura em rede local
- varredura em rede sem fio
- varredura a partir de rede externa

A Coleta Local

A coleta local consiste em usar um programa de busca de senhas local com a finalidade de ver quais senhas ou dados confidenciais estão armazenados no seu micro. Programas como o Cain e o Rock XP se prestam bem a esta tarefa:

http://www.oxid.it/cain.html
http://www.snapfiles.com/get/rockxp.html

Verifique suas opções de armazenamento de senha local e implemente algum tipo de proteção ao registro, como o oferecido por alguns programas. O System Mechanics por exemplo, pode ser útil para proteger o acesso ao sistema. Infelizmente as versões mais recentes tem causado problemas de travamento.

A Varredura Usando Loopback

Neste mesmo livro explicamos como usar um programa de varredura, o Languard, para buscar por máquinas vulneráveis. O mesmo programa pode ser usado apontando para a sua máquina. Mas qual é o IP da sua máquina local? O IP da sua máquina local é **127.0.0.1**, também chamado de **localhost** (host = máquina, ou seja, máquina local). Sabendo disso, agora é só digitar no Languard ou outro programa de varredura a palavra localhost ou o IP 127.0.0.1.

Você poderá testar o funcionamento de servidores Web ou de FTP rodando em sua própria máquina, através dos endereços:

http://127.0.0.1
ftp://127.0.0.1

O ping também funciona. Experimente entrar em uma janela de prompt e digitar ping 127.0.0.1. No Windows XP, faça assim:

Iniciar -> Executar - > digitar **CMD** e clicar em **OK**

Quando abrir a janela de prompt, digite:

ping 127.0.0.1 ou **ping localhost**

Uma variação do comando acima é:

Iniciar -> Executar - > digitar **ping localhost -t**

Para encerrar pressione **CTRL + C**.

Quando o Languard ou qualquer outro programa de varredura apresentar o relatório, você deve investigar cada alerta individualmente e tomar as medidas necessárias para corrigir cada um dos problemas apresentados. Isto vai exigir um pouco mais de conhecimento sobre sistema operacional do que o usuário típico costuma ter.

A Varredura em Rede Local

A varredura em rede local, além dos procedimentos descritos anteriormente, deve incluir um sniffer para ver a quantas anda a suscetibilidade da sua máquina à captura de dados trafegando na rede.

A varredura em rede local obviamente vai necessitar de uma segunda máquina conectada diretamente por um cabo de rede do tipo crossover ou usando um hub, caso possua mais de dois computadores na rede.

O que difere a varredura em rede local da varredura por loopback é que o micro local pode ser vulnerável na rede e o loopback não revelar isso. Até por conta do relacionamento de confiança que uma varredura por loopback encontra.

Outro ponto a ser observado é que o micro a ser testado na varredura em rede local não vai ser localizado pelo IP 127.0.0.1. Este IP (ou o nome *localhost*) se refere a máquina local. Todas as máquinas da rede possuem o seu próprio IP 127.0.0.1. O IP da máquina a ser testada na rede deverá ser descoberto usando a sequinte sequência de comandos:

Iniciar -> Executar -> Digitar **CMD** e clicar em **OK**

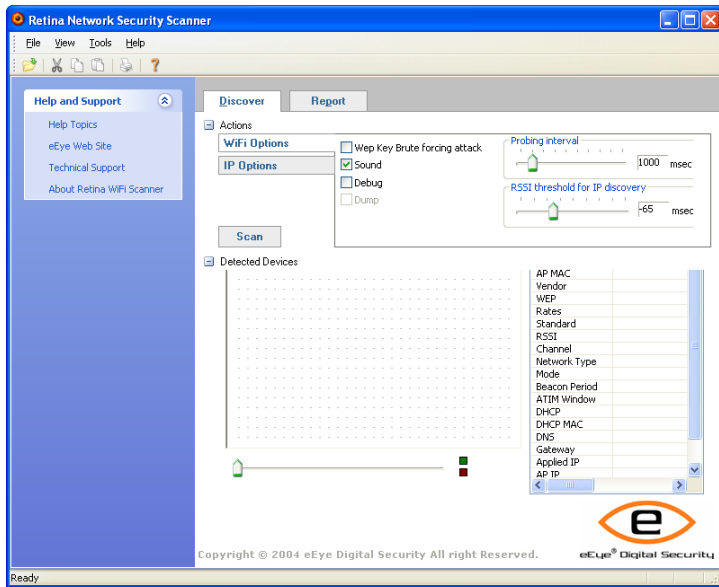
Na janela de prompt digite **ipconfig** para visualizar o IP da máquina a ser testada. Provavelmente será algo como 192.168.0.x ou 10.0.0.x, onde x é um número qualquer entre 1 e 255.

Varredura em Rede Sem Fio (Wi-fi, Bluetooth)
A varredura de rede sem fio vai precisar que pelo menos duas máquinas estejam conectadas por conexão Wi-fi ou Bluetooth. Existem programas de varredura específicos para redes sem fio, como a ferramenta gratuita Retina Wi-fi Scanner, que inclui uma versão para Pocket PC:

http://www.eeye.com/html/resources/downloads/wifi/index.html

Outros sites com ferramentas para varredura de redes sem fio:

http://www.wardrive.net/wardriving/tools
http://www.geschonneck.com/security/wireless.html

Além de verificar a vulnerabilidade da rede sem fio, é importante que também seja verificado o alcance do sinal. Isto pode ser feito com um notebook e uma antena mais potente, como a cantena, ou algum modelo de antena quadrática ou parabólica.
O principal problema das redes sem fio é a configuração aberta e a criprografia desabilitada. Fixe sua atenção nestes dois pontos pricipais. E no caso da criptografia, prefira o protocolo WAP. Ao contrário do que ocorre com as senhas de e-Mail, os ataques de força bruta ao protocolo WEP tem sido bem sucedidos.

Varredura a Partir de Rede Externa

A varredura a partir de rede externa pode ser feita antes e depois dos outros procedimentos descritos. Agindo assim você terá uma idéia de quais alterações foram úteis. O Languard porssui uma opção de comparação de relatórios. Clique em ***Tools* -> *Result comparison***.

A varredura a partir de rede externa é a mais próxima dos ataques que você se sujeita na Internet. Este procedimento depende da máquina a ser testada e da máquina invasora estarem conectadas ao mesmo tempo na Internet, sem nenhum tipo de vínculo. Seja em forma de rede local ou de compartilhamento da Internet.

Talvez esta seja a maior dificuldade: ter duas máquinas com duas conexões distintas. Entre as opções para conseguir realizar este tipo de teste, podemos sugerir a parceria com alguém que possa ceder o uso de outra máquina conectada para esta finalidade. Para saber qual é o IP externo da sua máquina, visite o site: **www.cursodehacker.com.br/ip.asp**.

O IP que vai aparecer é o que deve ser informado no programa de varredura.

Conclusão

As novas tecnologias têm obrigado a nós autores experimentarmos outras formas de comunicação com nossos leitores. O formato que tenho usado é do livro com vídeos para assistir na tela do computador e mais recentemente o DVD. Mas acredito que a maior conquista dos leitores atuais é poder falar diretamente com o autor, seja por e-Mail, programa de mensagem instantânea ou telefone.

E não é só isso, antes de adquirir um livro é possível a qualquer pessoa obter informações sobre a obra e sobre o autor. Livros que prometem e não cumprem são desmascarados em pouco tempo.

Por outro lado, quando o livro é bom, costuma gerar comunidades no Orkut, grupos no Yahoo! e com um pouco de *sorte*, vai parar em uma destas redes de troca de arquivos. Este livro está nascendo hoje e não sei o que o futuro reserva para ele. Espero que agrade, pois ainda tenho os volume dois e três para lançar até o final do ano.

Antes de ser autor, também sou leitor. E o que me levou a ser autor, foi a insatisfação com o que encontrei nas livrarias. E isto não é de agora. Por volta de 1984 eu mandei uma carta a uma editora, cujo nome não recordo, reclamando do livro "Os Melhores Jogos para TK-2000".

A resposta que recebi foi um convite para escrever um livro melhor. Na época eu não tinha competência para escrever sobre programação de jogos, mas fiz o que sabia e surgiu o livro "Programação Assembly para TK-85". Não perca tempo procurando este livro. Depois de algumas semanas datilografando, descobri que o mercado não estava receptivo à linguagem assembly para micros Sinclair.

Então escrevi um livro com listagens de programas de informática para eletrônica. Eu estava lotado na Polícia Rodoviária e demorei tanto a entregar este livro que o saudoso Gilberto Afonso Pena, editor da revista Antenna-Eletrônica Popular (**www.anep.com.br**), achou mais conveniente publicá-lo na forma de artigos na revista.

Quer dizer que minha segunda tentativa de virar autor também não deu certo. Para encurtar a conversa, só consegui publicar meu primeiro livro alguns anos depois e mesmo assim sobre um tema bem diferente da minha especialidade atual. Meu primeiro livro foi publicado pela extinta editora Cátedra, não tinha nem sessenta páginas e era sobre cânticos africanos

traduzidos do dialeto quimbundo para o português. Fez muito sucesso na época e me deu a oportunidade de iniciar uma carreira como produtor de eventos e apresentar um programa de rádio na Metropoliana AM - 1090KHz e depois na Mauá-Solimões AM - 1480KHz.
O maior desafio que tive e que prorrogou bastante minha entrada no mercado editorial, veio da família. Passar o dia em casa escrevendo na hora que desse na telha e ainda viver disso? Não foi fácil convencer o pessoal lá em casa. Era só sentar diante do computador com a máquina de escrever ao lado para ser ofendido de todas as formas. Só depois de me estabelecer como empresário é que pude voltar a minha maior missão.
Mas se tem uma coisa que aprendi durante todos estes anos é que nós nos tornamos o que somos, independente do boicote das outras pessoas, incluindo familiares munidos da melhor das boas intenções.
Relato este episódio, pois espero que ele lhe seja útil de alguma forma. Se você tem um sonho que acha impossível, se você trabalha em algo que não lhe dá satisfação pessoal, pense assim: “o Marco Aurélio conseguiu, então eu também posso conseguir”. Você só precisa descobrir seu próprio caminho e seguir por ele. No mais é boa sorte e até o volume dois, com novas técnicas sobre o tema segurança na Internet.

(a) Prof. Marco Aurélio Thompson
http://MarcoAurelio.Net

Fale Conosco

É como eu já disse, o maior benefício à disposição dos leitores atualmente é poder entrar em contato direto com o autor, seja para tirar dúvidas ocorridas durante a leitura, contestar informações ou oferecer valiosas contribuições, em forma de sugestões para as futuras edições da obra. Os meios de contato comigo são estes:

Site

http://www.cursodehacker.com.br

e-Mail

atendimento@cursodehacker.com.br

Telefone

(71)8108-7930
(21)2231-2899

Projeto Livro Grátis

Como forma de agradecimento aos meus milhares de leitores, estou disponibilizando para download, livros gratuitos em formato eBook. Informações no site www.cursodehacker.com.br.